Exhibit C

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION, Plaintiff, v. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendant.	CIVIL ACTION NO. 1:20-cv-12090-DPW

DEFENDANT'S TRIAL AFFIDAVIT OF CRAIG SMITH

I, Craig Smith, hereby declare and say as follows:

I. Background and Experience

1. I have over 20 years of experience in the security industry, covering a broad range of security areas. My experience includes reverse engineering, hardware circumvention techniques, code analysis, penetration testing, network protocol analysis, exploit development, software lifecycle development, and management of full security teams. A true and accurate copy of my curriculum vitae is marked as Exhibit 519 and attached hereto.
2. I received an associate degree in computer programming from Cincinnati State Technical and Community College in 1996.
3. From 1998–2001 I worked at Cincinnati State College as a Network Administrator. In this role I ran the college's network and managed classroom infrastructure.

4. From September 2001–November 2002 I worked as a Senior Security Analyst at Cardinal Solutions Group. In that role I served as a consultant for several healthcare and medical facilities, and served as part of the core security team performing incident response, forensics, and network architecture.

5. From November 2002–March 2003 I worked as a Network Security Engineer at Maximize I.T. In this role I built their flagship Intrusion Detection Service (IDS). Their Intrusion Detection Service was based on an open source IDS called Snort. I modified the Snort IDS and submitted patches back to the open source project and was listed as an official author. My main role was to build a machine learning algorithm around Snort to sort through falsely detected incidents.

6. From March 2003–March 2007 I worked as the Lead of Security Operations at Great American Insurance. In this role I installed, maintained, and administered over 20 enterprise firewalls, administered authentication services, wrote custom IDS signatures, and performed vulnerability assessments.

7. From March 2007–October 2008 I worked as a Senior Security Consultant at Neohapsis, Inc. Neohapsis was a boutique security company that performed offensive testing of networks for clients such as healthcare facilities, banks, prisons, and casinos. In this role I specialized in application assessment, binary analysis, and penetration testing. I conducted training on the Software Development Life Cycle (SDLC) and secure coding practices and contributed new tools to binary analysis and research.

8. From October 2008–January 2011 I worked as a Senior Reverse Engineer at Riverside Research Institute. In that role I specialized in reverse engineering and bypassing software

schemes, binary security assessments, malware analysis, and the development of custom tools to aid in analyzing, debugging, and bypassing software protections.

9. In 2012, I worked with Battelle, a private non-profit scientific and development research company, to educate students on how to assess vehicles to identify security vulnerabilities.

10. In 2012 I also started an open organization known as Open Garages, which is a distributed group of mechanics, performance tuners, artists, and security researchers that reverse engineer vehicles for the purposes of modifications, research, and repairs

11. From 2011 to 2016 I ran my own security company, Theia Labs, that covered advanced areas of cyber security. We specialized in developing antivirus heuristic engines for mobile platforms and hardware reverse engineering. Heuristical antivirus is a type of antivirus that can detect malicious content based on behavior. During my work at Theia Labs I focused on automotive cybersecurity for clients including automotive companies and tier suppliers. In this role I worked on many different components of vehicles, including telematics systems, gateways, immobilizers, tire pressure sensors, and infotainment centers.

12. Theia Labs was acquired by Rapid7 in 2016, and I worked for Rapid7 as the director of transportation security. The transportation security division handled cybersecurity for trains, planes, and automobiles. During my time at Rapid7 I worked on Metasploit, an industry standard security auditing and exploitation tool, to add hardware capabilities that included but was not limited to, automotive auditing and vulnerability scanning.

13. After leaving Rapid7 in 2018, I worked directly for Byton, an electric vehicle manufacturer, to run their security team and help develop secure gateways and telematics systems.

14. I started my current position as Senior Director of Security at Bird, a micro-mobility company, in 2019. In this role I lead Bird's information security teams and oversee the infrastructure security (servers, cloud services), application security, product security, and physical security. In this role I have built out an international security program that went from factory development to tracking a full set of key performance indicators (KPIs) for executive and board members. I oversee a global fleet of rental and retail vehicles and ensure compliance, security and budget are all aligned with the current business objectives.
15. I authored the Car Hacker's Handbook, a book that details how vehicle security works and describes how to perform threat models and perform reverse engineering and penetration testing on passenger vehicles.
16. The Car Hacker's Handbook is used as the textbook for an automotive cybersecurity course at Walsh University. I have spoken to the students in this class as a guest lecturer. I have also been a guest lecturer on this book at Dartmouth College in 2016 and the University of Maine in 2017. My guest lecturing focused on teaching vehicle security, CAN bus reverse engineering, and vulnerability detection.
17. I have been retained as an expert by the Office of the Massachusetts Attorney General and am being compensated at the rate of $250 per hour for my work in this case.

II. Opinion Summary

18. The technology exists for original equipment manufacturers (OEMs) to comply with the Requirements of the 2020 Massachusetts Right to Repair Law (RTR Law) without exposing consumers to increased security risks.

19. It is my opinion that it is possible for the OEMs to immediately comply with Section 3 of the RTR Law by disabling their telematics system. This is a short-term solution that would actually enhance overall vehicle cybersecurity.

20. In the medium-term, OEMs can comply with Sections 2 and 3 of the RTR Law by utilizing the existing J-1962 connector and a telematics dongle. The OEMs could continue using the J-1962 connector and a telematics dongle to comply with the law for as long as they like.

21. In the longer term, OEMs can adjust the vehicle network architectures on new vehicles to comply with the law by using a fully-telematic platform. OEMs can take as much time as needed to adjust the vehicle network architectures by either disabling telematics or using the J-1962 connector with a telematics dongle in the interim.

III. <u>Security Considerations, Vehicle Components & Terminology</u>

22. Automotive systems and architecture vary throughout every make, model and year. A vehicle architecture includes all the components, wiring, and the electronic makeup of the vehicle. Alfred Adams, Chief Product Cybersecurity Officer at General Motors (GM) described electrical architecture as "the set of components and connections of those components, the interfaces, to create an electrical system that delivers feature content for customers." Deposition of Alfred Adams, p. 8. Although automobile manufacturers sometimes use common vehicle designs to try to provide a generic architecture, such designs typically support a wide number of variants, each of which may have its own characteristics. Given the diversity of vehicle architectures, there are different security considerations for each vehicle depending on how it is designed. This diversity of vehicle

architectures also means that there are many different approaches that manufacturers can use to construct their vehicles to comply with the RTR Law.

23. When architecting security, security professionals need to consider many factors, whether the security is for a laptop, web server, cell phone, vehicle, or nuclear power plant. To evaluate these factors, the security team conducts a threat model of the target item that needs to be secure. A threat model is an analysis of a system to determine all the possible risks and rank them by severity. When the security team performs a threat model, they bring in representatives from different areas of the organization such as quality assessment, project managers, User Interface Designers, managers, as well as the engineers. Together the group maps out all the attacks that they can think of. The group then ranks each threat to determine the risk it presents. The scoring for ranking threats typically takes into account considerations such as: How dangerous would this threat be? How many people would this attack affect? How easily discoverable is this vulnerability? How hard would it be for an attacker to exploit this vulnerability?

24. Security professionals use the answers to these questions to provide a score for each identified threat to the platform. There are many attack scenarios that will arise in the threat modeling process that the company will not try to stop, because trying to stop every method of attack would hamper how a business works. This is one reason why people from different areas of the organization are consulted during this process to inform the security team — representatives from other areas of the organization can inform the security team whether a particular feature is more important to the product's capabilities than the perceived risk. Assemble the Threat Modeling Team

https://www.codemag.com/Article/0211091/Threat-Modeling] [Microsoft Introduction to Threat Modeling (slides)].

25. When a threat is identified that conflicts with the goals or requirements of the business, it is not an all-or-nothing situation. The security team will often take this information and work with engineers to come up with methods to mitigate but not necessarily eliminate the risk. The business accepts the risk, but limits the external risk or damage caused from a threat being exploited by adding mitigation techniques. To develop an effective mitigation strategy, the security team thinks about the threat actors, or the "bad guys," in the scenario. For the example of a telematics system, the threat actors would be an external hacker, using the telematics to interact with the vehicle without the owner's knowledge.

26. The security field uses technical terms that are often used interchangeably to discuss the same or similar concepts. The chart below lays out common security terminology used in the discussion of the security of a vehicle's architecture:

Security Term	Description
Encryption Keys, Certifications (Certs), Asymmetric Encryption	Public/Private keypairs. Used to verify content.
Gateway, Firewall, Segmentation, Isolation	A method of separating networks and controlling data flow.
Secure Boot, Secure Storage, Trusted Platform Module "TPM", Hardware Based Root of Trust	Using keypairs to store or verify digital content. A process to load/store keys and control who can add new keys.
Digital Signing	Using a key to sign a message
Unique IDs, Passwords, Seed-Key	Traditional security measures similar to a username and password. When newer architectures implement Encrypted Keys and Certification it often replaces the need for traditional username/seed key authentication systems.

27. Vehicles have several different internal components that control how the vehicle functions. The internal components vary between different types of vehicles.

a. <u>ECUS</u>

28. An internal computing device within a vehicle is generically referred-to as an "Electrical Control Unit" or "ECU." The number, scope, and layout of ECUs within a vehicle varies. In the past 20 years, it was common for a single ECU to govern the operation of multiple systems (such as brakes, steering, door locks, interior lighting, etc.). Currently, it is more common for a single ECU to govern operation of a single system, ranging anywhere from an airbag controller ECU to an ECU controlling the dome light of the vehicle.

29. The ECUs within different vehicle architectures vary. [redacted] Deposition of Kevin Baltes, 4.5.21, p. 185.

30. The GM vehicle network diagram below from the second page of the AAI-GM-0001585 document [redacted] A true and accurate copy of AAI-GM-0001585 is marked as Exhibit 11 and attached hereto.

[redacted]

31. Some ECUs that may appear in a vehicle include those listed in Slide 11 of Exhibit 10: AAI-GM-0001585, copied below:

[redacted]

32. The capabilities of different ECUs vary widely. Some ECUs are very simple and cannot even receive network upgrades. For instance, in the above diagram [redacted] Most ECUs of medium to high complexity are capable of receiving updates, typically by physically connecting a device to the OBD-II port or other location on the vehicle network. At least half the modules in the above list would fall into this category.

33. Where a vehicle has wireless connectivity, a complex ECU may be capable of receiving updates from a non-physical source (often called "over the air" updates). On its own, the particular functionality of an ECU does not indicate whether it would support over the air updates. Which ECUs support over the air updates is determined by the supplier, how capable the microcontroller is, and the requirements set by the OEM.

34. OEMs procure ECUs from suppliers such as Bosch, Denso, or Continental to match the functionality and rules the OEM needs to be supported by other vehicle components. Often a supplier has an ECU with base functionality that loosely matches an OEM's needs, and the OEM pays for additional customization. The OEM's rules may govern, for example, the authentication of messages, or the form of permissible messages communicated on the network to, from, or between specified ECUs. These communication rules typically are defined within a .DBC file (Vector proprietary format) or .ARXML file (Autosar XML format). These rules determine how different ECUs communicate with each other, which ECUs can communicate with other ECUs, and what type of communication is permissible between ECUs. These files are referenced internally for all business stakeholders, shared with suppliers, and used by third parties performing security reviews of existing and prototype ECUs.

35. Design and procurement of a new ECU, including appropriate testing, may take several years, in part because suppliers of ECUs require lead time to make significant changes to their products.

36. In contrast to creating an entirely new ECU, the time required to update an ECU for smaller changes, such as bug fixes, may be as little as a month, depending on the particular complexity and capabilities of the ECU. Some ECUs are so advanced they are basically a small computer. Most modern Infotainment Systems would be classified as one of these advanced ECUs. An ECU that supports over the air updates, such as a modern Infotainment System, can be updated within a month. For instance, on August 21st, 2019, the security researcher team 360 Group reported 19 ECU vulnerabilities on the Mercedes-Benz E Series, and Mercedes-Benz rolled out their first fix to 2 million affected vehicles

five days later. Lindsey O'Donnell, *Black Hat 2020: Mercedes-Benz E-Series Rife with 19 Bugs*, ThreatPost (Aug. 6, 2020), https://threatpost.com/black-hat-19-flaws-connected-mercedes-benz-vehicles/158144/.

b. Internal Networks

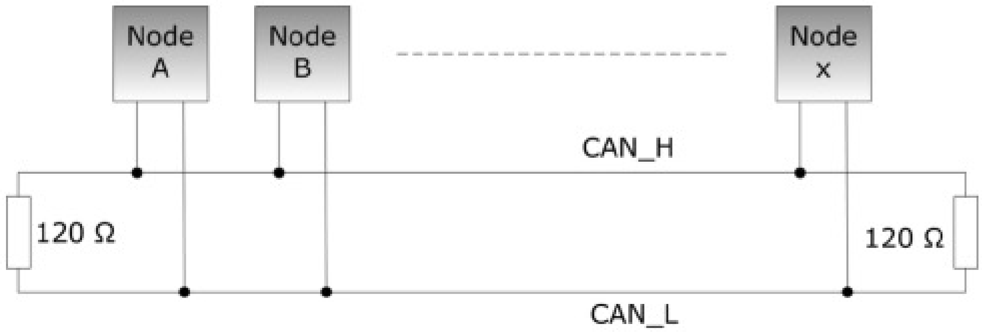
37. ECUs are connected to one another, and to other vehicle components, by networks. Although there may be many different types of communications networks within the vehicle, the most common one is referred to as a CAN bus network.

38. CAN bus is a two-wire network that became standard in 1997 and mandatory in 2008. CAN is a high-speed vehicle network that is resilient to electrical interference. CAN networks can be used for general communication between ECUs, diagnostics, software updates, and to run automated tests.

39. A CAN Packet is a message that travels over the CAN bus between ECUs within the vehicle. CAN Packets are also referred to as a CAN Frame. A CAN Packet typically holds 8 bytes of data, which is a very small amount. This is one of the reasons that CAN does not typically support encryption or authentication of individual packets.

40. A newer standard called CAN-FD supports 64 bytes of data and can be used for larger, faster transfers as well as supporting encryption and authentication services.

41. The following diagram shows a very simple, generic CAN bus network. Wilfried Voss, *CAN Bus and SAE J1939 Wiring Requirements and Trouble Shooting*, Copperhill Technologies (May 10, 2017), https://copperhilltech.com/blog/can-bus-and-sae-j1939-wiring-requirements-and-troubleshooting/. In the diagram, the "CAN_H" and "CAN_L" lines are the two wires of the CAN bus, and the "Nodes" represent the ECUs that are connected by the CAN bus.



42. CAN bus topology diagrams demonstrate which ECUs are connected on a specific CAN bus. Below is [redacted] provided by GM in AAI-GM-0001422. The boxes in the below diagram represent ECUs and the lines are the CAN bus wires connecting those ECUs. A true and accurate copy of AAI-GM-0001422 is marked as Exhibit 7 and attached hereto.

[redacted]

43. There are many other networks and buses that can be used within a vehicle other than CAN. Some examples include: CAN-FD, LIN, KWP, K-Line, MOST, FlexRay, and Ethernet.

These alternative networks are often selected based on their cost or speed. For example, LIN is a one-wire network, which means it costs half as much as CAN's cost to deploy. MOST is a plastic fiber optic line that can be more expensive, but offers much higher speeds than CAN. Ethernet is a newer network, while KWP is older but still used. Accordingly, whether these alternative networks are used depends on several factors, including the year a vehicle was built and the features of a particular vehicle.

44. Each of these networks has a method to perform diagnostics and set configuration controls.

45. Configuration controls define any method for setting specific configuration for an ECU. Configuration controls could range from configuring fuel map settings to assigning a new tire pressure sensor.

46. For CAN-based networks, the diagnostic communication happens over a standard called Unified Diagnostic Services (UDS). The UDS standard is what diagnostic scan tools (devices which connect to a vehicle through the OBD-II connector to perform diagnostic functions) primarily utilize for communications to the different ECUs within a vehicle. This standard allows components in different makes, models, and years to have a standard way to communicate diagnostic information.

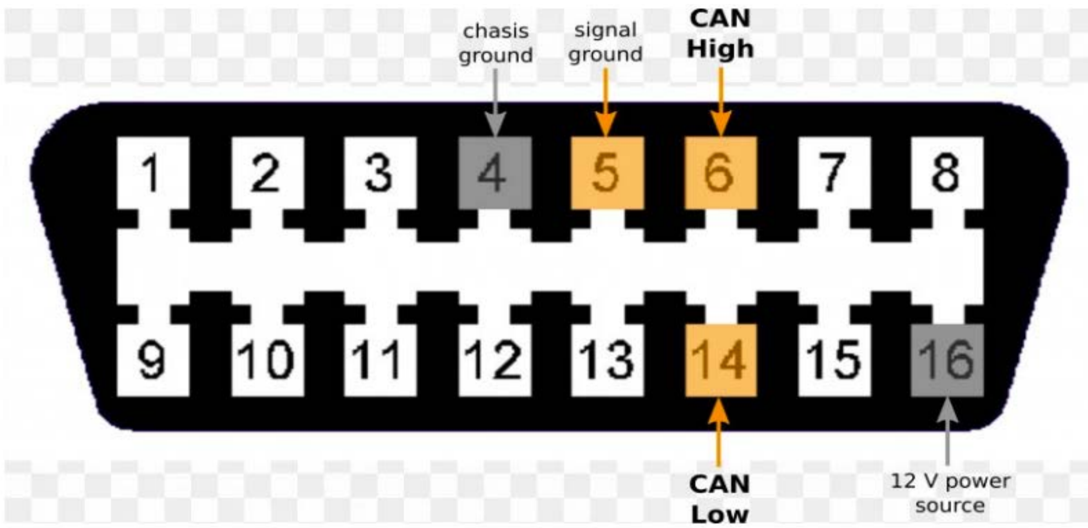
47. Like UDS for CAN Bus, each different type of network has a corresponding diagnostic system. Sometimes, a vehicle is designed to use a gateway (explained in greater detail in paragraph 74) to relay diagnostic information to/from ECUs that are not connected directly to the OBD connector, but are connected to other bus networks.

c. <u>The On-Board Diagnostic System</u>

48. The diagnostic connector, often referred to as the DLC (Diagnostic Link Connector) or OBD-II, became a standard around 1996. It is formally called the J-1962 connector, which

refers to the SAE standard that provides the required standardized format for the pins on the port. Each pin on the port is reserved to perform a different function.

49. This diagram shows the J-1962 connector. The colored and labeled pins on the diagram are the only ones that are standard, and the other pins can vary for each make, model, and year of vehicle.



https://favpng.com/png_view/car-car-on-board-diagnostics-pinout-obd-ii-pids-wiring-diagram-png/04igebfi.

50. Federal regulations require emissions-related data to be made available through the OBD-II port.

51. While the OBD-II port has become the access point commonly used to access non-emissions-related diagnostic, maintenance, and repair information using a diagnostic scan tool, each OEM decides which information is available through the unregulated pins on the OBD-II port. Because the OBD-II port is only required by regulation to provide emissions-related data, electric vehicles, which do not produce emissions, generally do not utilize the

OBD connector. In place of the OBD-II port, most electric vehicles use a proprietary connector for diagnostics.

52. By providing a standard method to communicate with the vehicle, the OBD-II port has greatly improved the availability of diagnostics and repairs for the consumer. Individuals or independent mechanics can use diagnostic scan tools, devices which connect to the vehicle through the OBD-II connector, to query the vehicle's different ECUs to determine if any Diagnostic Trouble Codes (DTCs) show that problems have been triggered in the vehicle. Scan tools can also gather additional diagnostic information from various ECUs to build a bigger picture of what could have caused a DTC. Diagnostics also record "freeze frame" data, which is a snapshot of data conditions as of the time when the DTC was triggered and often contains information such as engine load, RPMs (Revolutions Per Minute), engine temperature, vehicle speed, and other vehicle conditions. Scan tools can also perform tests necessary for diagnosis and repair, such as running a vehicle through a set of routines to ensure proper working conditions. An example of such a test is a "gauge sweep" test, which moves all the gauges (such as the speedometer) to max and return, in order to verify the gauges do not get stuck and have full sweeping capabilities.

53. Advanced diagnostic tools can write and modify data in order to fix or correct a problem with the vehicle. Writing data in this context refers to changing configuration settings or memory contents. For instance, when the size of the tires on a vehicle are changed, the axle parameters need to be updated so the ECU can properly calculate the tires' revolutions. These updates are important for accurate odometer readings, anti-lock braking calculations, and speed and performance calculations.

54. The information I reviewed in this case shows [redacted] Deposition of Kevin Baltes, 4.15.21, pp. 136-42.

55. These diagnostic functions are predefined in the software of the vehicle's ECUs when the vehicle is built. It is also possible to update the ECUs of a vehicle that is in the field to accommodate new diagnostic functions.

56. Execution of a diagnostic function may be made subject to a condition specified by the OEM and built into the vehicle's firmware. For example, [redacted] Deposition of Kevin Baltes, 4.15.21, p. 154.

57. A common rationality check is that the propulsion system is not active, or that the vehicle's speed is below a certain speed. Rationality checks are coded into the applicable ECU and can be used in a Boolean fashion.

d. <u>Telematics Systems</u>

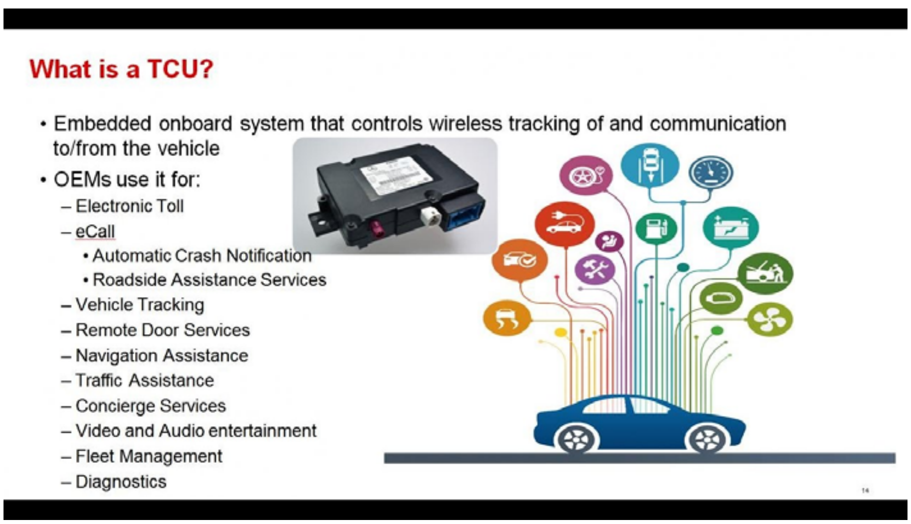
58. Many late-model vehicles are connected with a telematics system, sometimes referred to as a "Telematics Control Unit" or "TCU." Telematics devices have "phone home" capabilities that can use either a WiFi or a Cellular signal to contact a "backend" network controlled by the OEM.

59. The vehicle can use these telematic capabilities to transmit information such as DTCs or communications from other devices. The vehicle can also use these telematic capabilities to receive information, such as over the air updates to ECUs or commands to perform actions such as lock or unlock the vehicle, stop the vehicle, or track its location. A

telematics system can potentially send or receive any information that can be sent or received while physically connected to the vehicle.

60. Telematics systems are often a separate ECU that is either connected to the vehicle's Infotainment System or attached to the main CAN bus network. When a telematics system is not a separate system, it typically resides within the Infotainment System. An Infotainment System (sometimes called an "IVI") is a modern adaptation of a "radio" that often has more capabilities such as maps, voice assistance, diagnostic information, and general automotive controls.

61. Some common uses for telematics are documented by Texas Instruments, a global semiconductor design and manufacturing company that makes integrated circuits and processors, in the image below:



Texas Instruments, *The Future of Telematics: What Lies Ahead for the Connected Car*, YouTube (Sep. 29, 2017), https://www.youtube.com/watch?v=ib7m-mnclsw.

62. Since 2015, GM has installed a telematics system called "On-Star" on every vehicle sold through typical consumer channels. Plaintiff's First Supplemental Responses to Attorney General Maura Healey's First Set of Interrogatories, 3/9/21. A true and accurate copy of

Plaintiff's First Supplemental Responses to Attorney General Maura Healey's First Set of Interrogatories is marked as Exhibit 515 and attached hereto.

63. Fiat Chrysler Automobiles (FCA) has at least had the option of including telematics since 2013, and after 2018 all vehicles include telematics. Exhibit 515: Plaintiff's First Supplemental Responses to Attorney General Maura Healey's First Set of Interrogatories, 3/9/21.

e. Telematics System Security

64. Adding telematics systems to a vehicle increases the vehicle's "attack surface" — that is, the external-facing area of opportunity that an attacker has to find vulnerabilities on a system, and thus are available to an attacker to find a vulnerability. Before telematics systems were added, a vehicle's attack surface was the physical vehicle itself, and security threats and risks required an attacker to be local to the vehicle. With the addition of a telematics system, the vehicle's inbound and outbound wireless communications became part of the attack surface.

65. With the addition of telematics systems to vehicles, in order to protect the consumer from an untrusted third party modifying or controlling their vehicle, it became important to have protections put in place on the vehicle's wireless communications. This protection has typically been achieved by adding encryption and segmentation to the vehicle network.

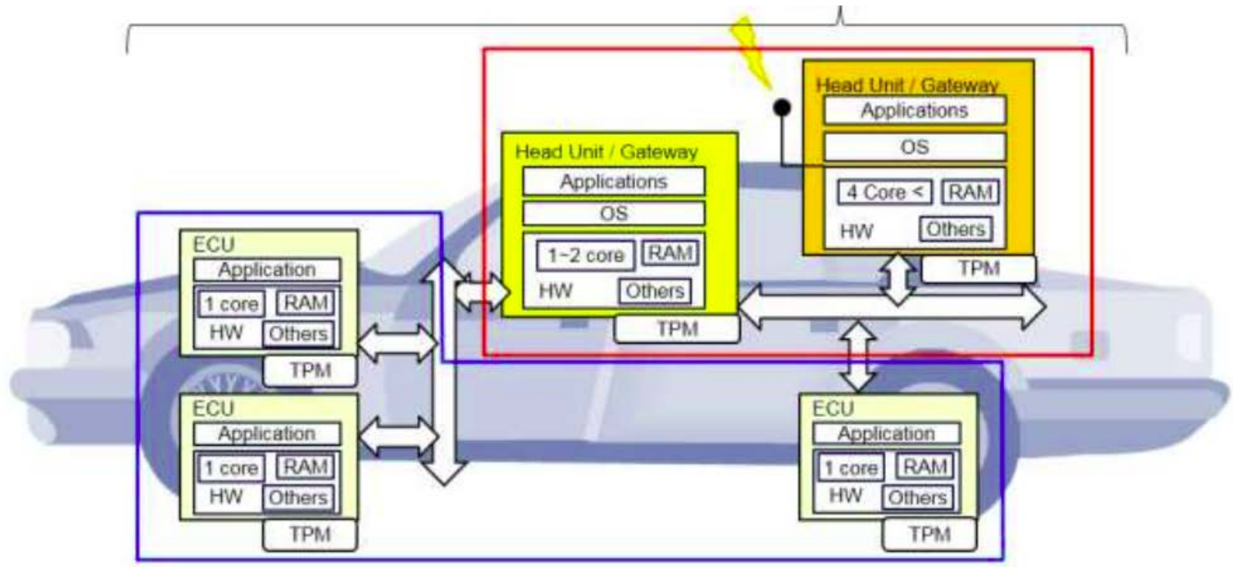
i. Encryption

66. Encryption keys can be used to ensure that digital content has come from a known source and has not been modified in transmission. At a high level, this works by breaking up keys into a public key and a private key, also known as a keypair. Public keys can be distributed and are not secret, while private keys need to be kept secret in order to be effective. When

sending digital content, the sender uses the private key to sign the content, then the receiver can use the public key to verify the message was signed by the private key holder and has not been altered.

67. To handle advanced security encryption and keys, vehicles typically store encryption keys on a special secure chip within that ECU called a trusted platform module or "TPM." Originally, the concept of TPM was created in China and was later globally standardized by the Trusted Computer Group that created the Trusted Cryptography Module, TCM. Traditionally, keys held by a TPM validate and approve messages for telematic communications and software updates. Those keys can also be used to validate and approve CAN packets, although that use is rare because it greatly expands the bandwidth requirements of the CAN network. TPMs can be configured so they are very hard to update remotely, in an effort to prevent hackers from remotely updating keys.

68. Below is a basic diagram showing an example of ECUs that contain a TPM. The yellow ECUs on the diagram represent the "head unit/gateway," which are typically more capable systems that can handle advanced encryption controls. The white ECUs on the diagram represent ECUs with a simplified subset of capabilities. The blue and red boxes on the diagram represent a possible segmentation between advanced TPMs and more simplified TPM networks. In this diagram, the "Head Unit/Gateway" ECUs represent the infotainment, telematics, and gateway/firewalls.



TCG TPM 2.0 Automotive Thin Profile For TPM Family 2.0; Level 0, Specification Version 1.01 Revision 15, TCG (May 31, 2019), https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM_2.0_Automotive_Thin_Profile_v1.1-r15.pdf.

69. One complexity with using TPMs to store keys is key management. If a key gets lost or leaked it can be very difficult to update these systems. Even large security companies have had their keys leaked in the past. For example, NordVPN had its private keys leaked, and the Trusted Computer Group that created TCM was originated by several companies including Intel, AMD, IBM, Microsoft, and Cisco— Intel, Microsoft, and Cisco have all had their private keys leaked for core security programs in the past. Dan Goodin, *Hackers Steal Secret Crypto Keys for NordVPN. Here's What We Know So Far*, Ars Technica (Oct. 21, 2019), https://arstechnica.com/information-technology/2019/10/hackers-steal-secret-crypto-keys-for-nordvpn-heres-what-we-know-so-far/; Lindsey O'Donnell, *Newest Intel Side-Channel Attack Sniffs Out Sensitive Data*, Threatpost (Mar. 8, 2021), https://threatpost.com/intel-side-channel-attack-data/164582/; Matthia Gliwka, *Microsoft Leaks TLS Private Key for Cloud ERP Product*, Medium (Dec. 7,. 2017), https://medium.com/matthias-gliwka/microsoft-leaks-tls-private-key-for-cloud-erp-

product-10b56f7d648; *Cisco Subdomain Private Key Found in Embedded Executable*, Slashdot (June 20, 2017), https://it.slashdot.org/story/17/06/20/1526259/cisco-subdomain-private-key-found-in-embedded-executable.

70. There are even companies such as Texplained that specialize in decapping chips to extract private keys. *IC Inside Lab,* Texplained, https://www.texplained.com/icinsidelab/. Decapping is the technique of removing the casing of a circuit board's chip and directly reading the transistors of the chip to reverse the code and extract sensitive information.

71. TPM systems used by Secure Boot are often viewed as a magical system to secure keys, but in actuality they do not provide additional security and are often used to restrict the use of a device to only OEM-approved actions. The problem with public/private key encryption is that private keys must be kept secret, but by including them in a consumer device they are at risk of being exposed.

72. One method to try to mitigate this problem and hide private keys is to include them in a TPM chip. But this method does not actually provide additional security, because there are several known ways to extract these secret keys, like using services such as those provided by Texplained.

73. In addition to not providing additional key security, including private keys in a TPM chip limits the ability to update private keys to the OEM. By allowing only the manufacturer/OEM to update keys, hardware security on keys prevents consumers from making changes under the guise of security.

ii. Segmentation

74. In addition to, or instead of, TPMs, some OEMs have built gateways around the OBD-II connector to limit threats from devices plugged into the OBD-II connector. A gateway is

a component that segments a network or devices from another network or device. Gateways may utilize keys or TPMs, but can also just be simple routing systems that move packets from one network to another. Gateways are similar to a traditional network firewall where network packets (i.e., CAN Packets) can be prevented from transferring to another network.

75. Some OEMs have segmented their internal vehicle network in an attempt to keep critical systems on a separate network than their more vulnerable ECUs that have a high attack surface or have been identified during a threat assessment to have increased risk of attack.

76. GM's stated security strategy [redacted] The image below from AAI-GM-0001192 shows [redacted] A true and accurate copy of AAI-GM-0001192 is marked as Exhibit 6 and attached hereto.

[redacted]

77. General Motors' Director of Product Cybersecurity discussed several other relevant security features that GM already uses and which could still be employed: disabling ports,

removing symbols from the software, data encryption, isolation within the component when using hypervisors and other methods, physical separation of the different chips in the component, removing labels from chips, and Address Space Layout Randomization (ASLR) stack canaries. Deposition of Kevin Baltes, 4.15.21, pp. 105–06. These security features can be implemented by any device, and are not related specifically to telematics or any technology unique to GM. This long list of security controls protects from a wide variety of different types of attacks, including on telematics systems.

IV. <u>Compliance with Section 3 By Disabling Telematics</u>

78. An immediate way for OEMs to comply with Section 3 of the RTR Law is to disable the telematics systems of newly-sold vehicles until they can design and implement a method of equipping vehicles with an inter-operable, standardized, and open access platform that can securely communicate all mechanical data emanating directly from the vehicle.

79. Section 3 of the RTR Law requires an OEM that sells vehicles in Massachusetts to equip those vehicles with an inter-operable, standardized, and open access platform if the vehicle "utilize[s] a telematics system." The RTR Law defines "telematics system" as: "Any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such information, in this chapter referred to as 'telematics system data,' utilizing wireless communications to a remote receiving point where it is stored."

80. This is a somewhat narrow definition of telematics, under which not every possible feature would constitute a "telematics system" as it's defined. For example, a video and audio entertainment function may just use telematics to play a Netflix application; this type of telematics use, which only includes inbound communications, would not fall into this definition of "telematics system." Even for telematics systems that collect and wirelessly

transmit information generated by the operation of the vehicle to a remote receiving point where the data is stored, disabling the remote transmission and storage of data from the vehicle is technologically feasible and can be done quickly.

81. The Plaintiff in this case has admitted that their representative OEM members are utilizing telematics for vehicle data collection used to make diagnostic decisions. Exhibit 515: Plaintiff's First Supplemental Responses to Attorney General Maura Healey's First Set of Interrogatories, 3/9/21.

82. GM's interrogatory response provides: "OnStar is a conduit to communicate with GM vehicles. OnStar transmits vehicle system information — including information that a customer may use to determine the necessity for maintenance, diagnosis, or repair — to customers and to GM. The scope of these transmissions have expanded over time, and have changed as vehicle capabilities have changed." Exhibit 515: Plaintiff's First Supplemental Responses to Attorney General Maura Healey's First Set of Interrogatories, 3/9/21.

83. FCA's interrogatory response provides: "FCA telematics units externally transmit data that a customer may use to determine the necessity for maintenance, diagnosis, and repair. This data is generated by the FCA vehicles' Service Quality Data Feed (SQDF), including data regarding mileage, emissions, tire pressure, trouble/error codes, engine performance, and fuel data. The SQDF sends immediate notifications regarding vehicle status to FCA, and it regularly collects vehicle status statistics that are sent in a monthly report to FCA, and then to customers via email." Exhibit 515: Plaintiff's First Supplemental Responses to Attorney General Maura Healey's First Set of Interrogatories, 3/9/21.

84. According to the Plaintiff's Supplemental Response to their First Set of Interrogatories, all vehicle telematics systems can be disabled. Exhibit 515: Plaintiff's First Supplemental Responses to Attorney General Maura Healey's First Set of Interrogatories, 3/9/21.

85. GM already has documented procedures for disabling its On-Star telematic services via an over the air signal. The On-Star telematics services can also be disabled in-person, manually, by modifying the hardware. Exhibit 515: Plaintiff's First Supplemental Responses to Attorney General Maura Healey's First Set of Interrogatories, 3/9/21, p. 12.

86. FCA has a procedure to opt-out of telematic data collection but claim they currently do not have a method to disable telematics. Exhibit 515: Plaintiff's First Supplemental Responses to Attorney General Maura Healey's First Set of Interrogatories, 3/9/21, p. 12.

87. There are at least three ways OEMs can disable their telematics' systems: (1) by modifying the configuration, (2) by disabling the "dialing services" that control external communication, or (3) by disabling the cellular access via the telematics provider.

a. <u>Modifying the Configuration</u>

88. One way OEMs can disable their telematics' systems is by modifying the configuration.

89. A configuration is a group of settings or scripts that tell the telematics system how to perform and connect to the backend servers run by the OEM.

90. To modify the configuration, the OEMs could intentionally provide the vehicle with a telematic configuration that would not successfully connect to service.

91. For example, the configuration could be set to be intentionally invalid. If the configuration states an invalid connection, then the telematics system will not be able to connect and transfer data to a remote receiving point for storage, as required to qualify under the law's definition of "telematics system."

92. Another possible telematic configuration that would not successfully connect to service would be to configure the device to only use local/loopback addresses. If the configuration uses a local/loopback address, that means that the configuration tells the device to talk to itself and no other system, and thus the telematics device would not meet the RTR Law's definition of "telematics system."

b. <u>Disabling the Dialing Services</u>

93. An alternative approach the OEMs could take to disable their telematics system is to disable the dialing service.

94. The dialing service is a program or a section of code that controls the cellular or wireless modems. That service can also be disabled so that it does not start the modems that apply to the telematics system when the vehicle starts.

95. An OEM can provide the vehicle with a software or configuration update that prevents the dialing service from starting, either via an over the air update or a configuration change. Successfully disabling telematics will prevent all cellular and WiFi communications to the manufacturer, and thus the telematics device would not store data as required to be a "telematics system" under the RTR Law.

96. Another method to disable the dialing services is to remove the SIM card (Subscriber Identity Module) to disable the dialing service completely. A SIM card is the small card in a cellular phone that enables a phone to connect to the cellular network. Vehicles have a similar SIM Card, which, if removed, disables telematic capabilities. When the OEMs develop a system that is compatible with the RTR Law, the telematics system could be re-enabled in person by re-inserting the SIM card. This approach would work best for vehicles with a normal SIM card. If, instead of a normal SIM card, a vehicle has a newer type of

eSIM card, removing it would be more difficult because it would probably be soldered in, so OEMs could use a different technique to disable the dialing service for those vehicles.

c. Disabling the Cellular Access Via the Telematics Provider

97. Another approach for OEMs to disable their telematics system is to disable the cellular support via the telematic provider.

98. All cellular connections have a telematic provider such as Verizon, AT&T, etc. It is possible to work with the telematic provider to have vehicles' telematics service cutoff and disabled, much in the same way that your personal cell phone provider would stop your cellular service if you stopped paying your bill.

99. According to the deposition of Stephen McKnight, GM has discussed going over such a solution via tabletop exercise in the past. Deposition of Stephen McKnight, 5.6.21, pp. 59–60. A tabletop exercise is a practicing technique where an OEM will go through different scenarios and role-play different solutions for the problem.

100. Because this solution involves disabling at the telematic provider, it can be done without changes on the OEM side.

d. Impact on Consumer Experience

101. Whichever technique the OEMs employ to disable their telematics systems, disabling telematics does not need to be an all or nothing change. Disabling the telematics system would only need to disable the capabilities that would be used to connect back to the OEMs' servers, while other functionality within the Telematics ECU could continue working. Other wireless communications, such as the customers' KeyFob, GPS, AM/FM/XM Radio, Bluetooth, and tire pressure sensors would still be able to function because they do not transmit data to the manufacturer for analysis and storage.

102. Nevertheless, when the telematics systems are disabled it is possible the vehicle will lose some features. This is one reason why the difference between vehicle architectures is so important — each vehicle can offer different functionalities and add-ons for the consumer. Over the air updates would no longer be feasible because there would no longer be a connection to a wireless network that could facilitate the update. In addition, some OEMs offer optional customer services such as a phone application to unlock a vehicle, roll the windows down, remote start, or other services that are also found on the vehicle's KeyFob. The mobile application requires telematics to function, so while the telematics system is disabled the customer will need to use their KeyFob to perform these functions.

103. Another optional function that may be affected on some vehicles is the Access Point. An in-vehicle Access Point is a WiFi connection provided by the vehicle, much like a public WiFi access point at a coffee shop. When a passenger connects with their personal device to the access point, their data will travel through the access point onto the cellular network. From there it may route directly to the internet, or first go through the OEM's network. If the vehicle offers a vehicle-based Access Point, and the OEM processes or routes any of the vehicle owner's network packets through its own network (instead of just forwarding directly onto the cellular network), this may have to be disabled. If this is disabled, the customer would not be able to use the vehicle-based access point to access the internet with their mobile devices.

104. Depending on how an OEM runs their stolen vehicle tracking and remote disablement functions, these functions may also be affected by disabling telematics. If an OEM has designed their vehicles to route these capabilities through the OEM's network

and integrated these capabilities into diagnostics or remote data storage, then these functions will also fall within the definition of "telematics system" and will need to be disabled until the OEMs have developed a long-term fix. It is possible that the stolen vehicle tracking system routes to a third-party service that does not include diagnostic information, and is a separate service than what the OEM provides, in which case it would not be effected by disabling the telematics system.

e. Effect on Vehicle Security

105. Disabling the telematics system would not have a negative impact on vehicle security. Because a telematics system increases a vehicle's attack surface, disabling the telematics will not increase the security threat to the vehicle — it will actually *decrease* security threats.

106. While the telematics system is disabled, updates and patches to the vehicle will need to be done in person. All this would mean is that safety and security updates would need to be rolled out the same way they were before telematics systems were added to vehicles, and the same way that updates are still rolled out to vehicles without telematics systems.

f. Time Frame

107. Disabling telematics can be accomplished quickly. As evidenced by the Mercedes-Benz telematics update in response to the 360 Group's identification of vulnerabilities discussed earlier in this testimony, a change that disables telematics can happen in a week's time. Lindsey O'Donnell, *Black Hat 2020: Mercedes-Benz E-Series Rife with 19 Bugs*, ThreatPost (Aug. 6, 2020), https://threatpost.com/black-hat-19-flaws-connected-mercedes-benz-vehicles/158144/. The Mercedes-Benz updates demonstrate a series of

telematic patches which would have a higher complexity than simply disabling the telematics system. Therefore, disabling the telematics system could likely be accomplished in a very short period of time, estimated under 2 months.

108. For vehicles that are equipped to receive over the air updates, the instruction to disable the telematics system could even be sent over the air.

109. In the case of GM, which already has documented procedures for disabling its On-Star telematic services via an over the air signal, the telematics systems on its vehicles that can receive over the air updates could be done immediately. The second slide in the AAI-GM-0001687 powerpoint below shows, [redacted] A true and accurate copy of AAI-GM-0001687 is marked as Exhibit 12 and attached hereto.

[redacted]

110. If other OEMs do not have existing documented procedures for disabling their telematics systems, software-based over the air updates that disable the telematics system

can go through normal code testing requirements and be pushed out to the fleet once the new patches are verified as stable.

V. <u>Compliance with Section 3 by Equipping the Vehicle with a Platform</u>

111. Section 3 of the Massachusetts RTR Law requires a "platform" that must be interoperable, standardized, and open-access," as well as "capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform."

112. Based on my experience with vehicles and other technological systems, "platform" refers to the vehicle architecture and associated software/features.

113. The RTR Law also requires the platform to be "inter-operable." Based on my experience with vehicles and other technological systems, to be "interoperable" means a standard way to connect and communicate with the vehicle. An interoperable device is one that can be used regardless of the manufacturer. For instance, regardless of who makes a home electronic device, it is designed to always work with your power outlet.

114. The RTR Law requires the platform to be standardized across all of an OEM's makes and models. Based on my experience with vehicles and other technological systems, to be standardized means to follow a common and well documented method to perform the necessary actions such that there is a common, agreed upon way of communicating.

115. The RTR Law also requires the platform to be "open access." Based on my experience with vehicles and other technological systems, to be "open access" means to have a non-gated way to gain access to the data and capabilities. For instance, a popular telematics provider, GeoTab, provides open access to their telematics. Geotab defines open access as " . . . an open platform system allows our customers unfiltered access to the data

that is generated by their vehicles. This information can be viewed via our user interface, MyGeotab, our application programming interfaces (APIs) for back-end system integrations, and for sharing data to a third party to provide great insight into the data." Scott Sutarik, *Why Choose An Open Platform System for Fleet Management?*, GeoTab (June 21, 2018), https://www.geotab.com/blog/open-platform-system/#:~:text=Geotab%20is%20an%20open%20platform,it%20as%20you%20see%20fit.

116. An open access platform provides a common method for any company to participate in diagnosis, maintenance, and repairs. At the same time, an open access platform can still use security to ensure the safety and privacy of the consumer. For example, an open access platform can still use encryption and security keys.

117. Open access requires the platform and the mechanical data it communicates with to be freely accessible to the owner, without the OEM acting as a gatekeeper.

118. Section 3 of the RTR Law requires the platform to be "directly accessible by the owner of the vehicle through a mobile-based application and, upon the authorization of the vehicle owner, all mechanical data shall be directly accessible" by independent repair shops and dealerships. Based on my experience with automobiles and other technological systems, to be "directly accessible" means that the consumer will not need to go through the OEM to perform diagnosis, maintenance, and repairs. The consumer will only need to confirm they are the ones intending to perform the diagnostics, maintenance, or repair.

119. Finally, the RTR Law requires that "access" to the platform include "the ability to send commands to in-vehicle components if needed for purposes of maintenance,

diagnostics and repair." [redacted] Deposition of Kevin Baltes, 4.15.21, pp. 136-42.

a. <u>The Existing J-1962 Connector and an OBD-Connected Telematic "Dongle" Can Provide the Platform Required by the RTR Law</u>

120. One potential "platform" that can be used to comply with the Massachusetts RTR Law can be the SAE J-1962 connector. With the addition of an OBD-connected telematic "dongle," the J-1962 connector can meet all the requirements of the RTR Law.

121. This solution would likely take six months to one year to implement. This estimation is based solely on the technical requirements and utilizing an existing company that provides fleet management dongles with a good security posture. This estimate does not try to factor in inter-departmental or collaboration issues that may arise.

122. The J-1962 connector with a telematic dongle can securely communicate all mechanical data. A dongle is a device that plugs into a vehicle to provide additional functionality.

123. The J-1962 connector is already the standard interface for performing diagnostics. The current practice is for mechanics to plug a diagnostic service tool into the J-1962 connector to obtain DTCs and send any necessary commands for diagnosis and repair. As such, each OEM already has a defined set of DTCs and bi-directional commands that is available for performing diagnostics, maintenance, and repair on a given vehicle.

124. [redacted] Deposition of Kevin Baltes, 4.15.21, p. 261.

125. The J-1962 connector with a telematic dongle could be standardized to provide all mechanical data. The industry can utilize the Unified Diagnostic Standard (UDS) already used with the CAN bus network for much of this requirement. However, the industry would still need to address gaps in diagnostics information and repair methodologies.

126. The OEMs could utilize other industry standards such as SAE J-1939, a heavy trucking standard, to bridge the gap in standardization. SAE J-1939 is a protocol that runs on CAN and CAN-FD that is used to unify the different heavy trucking platforms. This allows for interoperability of parts and a consistent way to connect third-party devices such as telematics systems or dongles. The heavy trucking industry sells their vehicles to fleet managers who outfit the vehicles with different parts depending on the carrier's goals. Having a standard way that devices communicate reduces the need for .DBC and .ARXML files to be shared between carriers, suppliers and third parties. The OEMs do not necessarily have to adopt the SAE J-1939 standard, as J-1939 does not unify diagnostics because it uses proprietary messages, but it is one example of a standard that's already in widespread use in heavy trucks that standardizes the diagnostic information and repair methodologies that are not addressed by UDS.

127. A possible scenario to standardize the telematic dongle would be to use the existing UDS for diagnostics and standardize on normal communications in a similar manner to J-1939. Under this approach, the line between what should be considered a standard and what should be considered proprietary should be drawn based on what the dealer has knowledge of and can repair. The dealer's capabilities should have parity to third-party mechanics so that independent repair shops have access to all vehicle data necessary for diagnostics, maintenance, and repair. As long as the OEM can provide access to all mechanical data

emanating from the vehicle they would be able to keep any information not normally provided to dealerships as proprietary.

128. The J-1962 connector already provides an interoperable physical connection into the vehicle. The UDS protocol provides an interoperable method for performing diagnostics. Using the J-1962 connector would achieve inter-operability by making access to diagnostics, repair, and maintenance information uniform across the industry, using the same connector and methods to perform diagnostics and repair.

129. The J-1962 connector would be open access because it is a known and equally-accessible way to gain access to a vehicle's diagnostic functionality. As long as the OEM has not imposed a secure gateway, the OEM does not stand between the user and access to the vehicle's diagnostic functionality. Even where access to the J-1962 connector is protected by security such as Mode 27 or encryption certificates, access does not depend on the OEM specifically granting permission.

130. The kind of direct access required by the RTR Law can be achieved by plugging a dongle into the J-1962 connector and/or approving an on-screen prompt on the infotainment console. By connecting the J-1962 connector to a dongle that has telematic or mobile capabilities, a vehicle owner could use a mobile device to connect to the J-1962 connector for all mechanical data.

131. To make the J-1962 connector "directly accessible" through a mobile based application, the telematics dongle provider will create a bridge between the vehicle's diagnostics and the consumer's mobile device. This is fairly common in the automotive industry and standard in the heavy trucking industry. Companies like GeoTab base their business on providing telematic and diagnostic data for global fleets of vehicles. *Success*

Stories¸ GeoTab, https://www.geotab.com/success-stories/. For non-heavy trucking, there are already existing telematic dongle manufacturers, such as Voyomotive, that can perform some of the diagnostic functions. https://www.voyomotive.com/.

132. There are a few ways to grant access to telematics dongles using secure gateways styled like the GM Global B Architecture. Keys could be granted to the vehicle owners, who can in turn grant additional keys to their chosen repair shop. The repair shop could have a tool that requires the vehicle owner to login and validate ownership to enable the key's usage on the vehicle. Alternatively, the repair shop could have the necessary keys installed in a dongle that could access mechanical data by being physically connected to the vehicle, and which could be removed by the owner at any time. These approaches would not compromise security or increase vehicles' exposure to hacking, as they are simply utilizing the same security and access methods already built into the vehicle

133. The J-1962 connector with a telematic dongle would have the ability to send commands for purposes of maintenance, diagnostics, and repair.

134. Existing passenger vehicle dongles can currently send and receive information through the J-1962 connectors that do not have a limiting secure gateway attached.

135. For vehicles that include a secure gateway, the dongles can be provided with the appropriate access level requirements to perform send and receive capabilities (sometimes referred to as "read" and "write" requests) to the vehicle. In the case of a role-based key or certificate, a dongle could be issued a key to match the dongle's intended capabilities for diagnosis, maintenance, and repair.

136. Under Section 2 of the RTR Law, the issued key would need to be administered through an entity that is unaffiliated with an OEM. This unaffiliated entity could

authenticate the dongle, the customer, or both. The unaffiliated entity would also manage the certificate revocation list (CRL), which is a list of invalid certificates. Having the unaffiliated entity maintain the CRL allows them to invalidate certificates of tools that are no longer supported or that have had security vulnerabilities.

137. In newer systems, the J-1962 connector directly connects to the secure gateway. The secure gateway is connected to the majority of the networks within a vehicle, and can connect and route network traffic to the appropriate device on behalf of the SAE J-1962 connector.

138. The diagram below from Exhibit 10: AAI-GM-0001585 [redacted]

[redacted]

139. GM did not provide documents indicating their secure gateway routes network messages to specific ECUs. However, [redacted] Deposition of Kevin Baltes, 4.15.21, p. 177.

140. [redacted] AAI-FCA-0011090, p. 3. A true and accurate copy of AAI-FCA-0011090 is marked as Exhibit 8 and attached hereto.

141. Regardless of whether a vehicle has a secure gateway, there are other security measures in use by OEMs that limit independent repair facilities' access to data necessary for diagnostics, maintenance, and repair. Two such measures include ECU authentication and message authentication. These measures can stay in place if the OEMs choose to comply with the RTR Law using the J-1962 connector as the "platform" required by Section 3, so long as the authorization aspects of these security measures are administered by an entity unaffiliated with an OEM as required by § 2 of the RTR Law.

142. To fully support all mechanical diagnostics and repairs, independent repair shops and vehicle owners need to be able to perform three types of actions: (1) communicate through the gateway, (2) read and write diagnostic data to each ECU, and (3) transmit packets to the ECUs. Each one of these steps can be achieved in a way that preserves security and enables independent shops and vehicle owners to make necessary repairs.

i. <u>ECU Authentication Through the Manufacturers</u>

143. Each ECU has its own method to validate diagnostic and repair access. Deposition of Kevin Baltes, 4.15.21, p.120. This can be a traditional UDS request for SecurityAccess (the name of the UDS command to unlock diagnostic services through Mode/Service 27) using the seed-key approach, or one that also verifies keys and certifications. *Security Access Service Identifier (0x27): UDS* Protocol, PiEmbSysTech Embedded Research Blog, https://piembsystech.com/security-access-service-identifier-0x27-uds-protocol/.

144. Since each ECU checks the authorized level of access before allowing write access, attackers are prevented from accessing these diagnostic functions without the requisite authorization.

145. ECUs also check the vehicle's current state before allowing diagnostics. For instance, there are checks to ensure the vehicle is not moving before bleeding the brakes.

146. When accessing the ECU for diagnostics and repair, UDS is typically used. Diagnostic UDS actions have associated security levels. Diagnostic functions that do not require authorization are considered the default security level, which is also called "anonymous access." This level allows for querying DTCs, freeze-frame information, and general data about the ECU. A vehicle can have up to 63 additional security levels. *Introduction to UDS*, https://udsoncan.readthedocs.io/en/latest/udsoncan/intro.html. These security levels are defined by each OEM and can vary for each make, model, and year of the vehicle.

147. Not all DTCs are currently shared as part of the UDS standard. Below is an example from AAI-GM-0001283 [redacted]

[redacted] A true and accurate copy of AAI-GM-0001283 is marked as Exhibit 514 and attached hereto.

[redacted]

148. OEM-specific DTCs that are not accessible without increased authorization access are often provided to groups like the Equipment and Tool Institute (ETI), which then provide the information to scan tool companies. A similar system could continue under the RTR Law in which the OEMs provide the OEM-specific DTCs to an unaffiliated entity like ETI that then makes the information available to reputable telematics dongle and scan tool companies. However, another option would be to make all DTCs readily available through UDS, which would not affect a vehicle's intellectual property or the security or safety of the vehicle. Either option is possible, so it would be up to the OEMs to decide which to employ.

149. SecurityAccess levels are protected by certificates or private algorithms. Not all levels of security access are needed by repair facilities. The RTR Law only requires access to mechanical data, which is defined in Section 1 as "any vehicle-specific data, including telematics system data, generated, stored in, or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair, or maintenance of the vehicle." Access to any other functions could be protected behind higher levels of manufacturer authorization.

150. Security access administered by an unaffiliated entity such as ETI ensures secure but fair distribution of access as required by the RTR Law.

151. [redacted]. AAI-FCA-11200, Slide 21. A true and accurate copy of AAI-FCA-11200 is marked as Exhibit 9 and attached hereto. [redacted] Exhibit 9: AAI-FCA-11200, Slide 7.

152. In general, FCA has made design choices to unnecessarily limit open access solutions. [redacted]. AAI-FCA-0010947. A true and accurate copy of AAI-FCA-0010947 is marked as Exhibit 504 and attached hereto. UPTANE's documentation details two methods to protect hardware systems such as ECUs without restricting the vehicle owner or third party repair shops. https://uptane.github.io/papers/uptane-deployment-best-practices-1.1.0.html#user-customized-updates. Method 1 allows for a third party to submit firmware updates that are approved by the OEM's system and can be validated by certificates between the third party and the OEM. Method 2 allows for overriding the root of trust. This allows a customer to void the warranty and take full ownership of what code is installed. According to FCA's documents: "the third party MAY choose to override the root of trust for ECUs, provided that the OEM makes this possible. Specifically, the third party may overwrite the map and

Root metadata file on ECUs, so that updates are trusted and installed from repositories managed by the third party instead of the OEM. The OEM may infer whether a vehicle has done so by using its inventory database to see if the vehicle has recently been updated from its repositories. The OEM MAY choose not to make this option available to third parties by, for example, using a Hardware Security Module (HSM) to store Uptane code and data, so that third parties cannot override the root of trust." [redacted], Exhibit 9: AAI-FCA-11200, Slide 7, [redacted] Deposition of Stephen McKnight, 5.6.21, pp. 121–23. Though I cannot provide an opinion on the vendor without knowing which one FCA uses, [redacted] Deposition of Stephen McKnight, 5.6.21, pp. 121–22.

153. Though FCA did not provide specific documents reflecting additional technical details of its Secure Gateway system, it appears that if FCA's V-PKI was administered by an entity unaffiliated with the manufacturer and used by all OEM makes and models sold in the Commonwealth, it would be compliant with the RTR Law. The unaffiliated entity administering the V-PKI system would need to be set up as an Intermediate Certificate Authority that would verify that only legitimate users are being granted SecurityAccess. In addition, a good safety measure would be to hold in escrow a valid keypair that exists in

the root CA in case anything happens to the company. This will ensure that if a disaster were to happen to the OEM, such as the company going bankrupt or losing its keys, the vehicles would still be able to be repaired.

ii. <u>Message Authentication Through the Manufacturers</u>

154. Another security mechanism used by OEMs is Message Authentication to secure packet-level communications. This mechanism only allows ECUs with specially signed packets to transmit on the bus network. If a packet including a data request for the vehicle to share information or perform a function is sent over a dongle, it would be rejected unless the dongle has the ability to sign the CAN packets to match the expected Message Authentication scheme.

155. Message Authentication is used to ensure that network packets originate from a valid source. The goal of message authentication is to prevent an attacker from replaying or spoofing (faking) packets on a network.

156. However, message authentication, as administered by the OEMs, has the effect of prohibiting certain testing of replacement components necessary to complete a repair. Because this functionality is very important for repairs, a method needs to exist outside of initial manufacturing to allow for access to test replacement components. Authorization for the SecurityAccess level necessary to perform Message Authentication capabilities can be provided to only verified owners and independent repair shops by using an unaffiliated entity to enable some of these types of features.

157. [redacted] AAI-GM-001584, [redacted]

[redacted]

A true and accurate copy of AAI-GM-0001584 is marked as Def.'s Exhibit H and attached hereto. These issues would arise because each ECU has its own unique security key. If a part is moved, it will need a new key that can only be issued with online connectivity. This would also apply to any third-party device made for a vehicle. To move parts or create alternative parts, a third-party group will need to be set up to issue keys.

158. Key Generation, the process through which a third-party group can issue keys, takes the ECUs unique ID and creates a key with a SUPPLIER_GEN_KEY, [redacted] Exhibit 10: AAI-GM-001584:

[redacted]

MASTER_ECU_KEYs can be generated by an unaffiliated entity by means of a special SUPPLIER_GEN_KEY intended to be used by the entity.

159. [redacted] An API Server is an Application Programming Interface (API) which is a gateway to bridge two pieces of software. The below diagram from Def.'s Exhibit H: AAI-GM-0001584 [redacted]

[redacted]

160. In addition to part swapping or installing new components, an important part of diagnosis, maintenance, and repair is to test and troubleshoot a vehicle. This is done by building a test bench. A test bench is created by connecting just a few selected ECUs. It is common to generate network packets for devices that are not connected (this process is called spoofing) to simulate the rest of the vehicle or a simulated condition.

161. [redacted] shown in the picture below from Def.'s Exhibit H: AAI-GM-0001584:

[redacted]

162. Requiring this capability for independent repair facilities and vehicle owners would not mean that the OEMs would have to support third-party components, since unauthorized parts would violate a vehicle's warranty. After a vehicle's warranty has expired, however,

the aftermarket often uses third-party components, and thus, to provide the access necessary for diagnosis, maintenance, and repair of a vehicle throughout the vehicle's life, the OEMs would need to support the existence of third-party components by using an unaffiliated entity to issue keys.

iii. <u>Manufacturer Authorization Under the J-1962 Method of Compliance: FCA Secure Gateway Updates for Compliance with Section 2 of the RTR Law</u>

163. The J-1962 connector is the existing method of access to the vehicle on-board diagnostics system under Section 2 of the RTR Law. Therefore, if OEMs choose to make the "platform" in Section 3 of the RTR Law the J-1962 connector, the RTR Law's Section 2 requirements also become relevant. Section 2 requires "motor vehicle owners' and independent repair facilities' access to vehicle on-board diagnostic systems" to be "standardized and not require any authorization by the manufacturer, directly or indirectly, unless the authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer."

164. Currently, some OEMs employ a secure gateway to manage authorization of third-party tools and mechanics.

165. [redacted] Exhibit 9: AAI-FCA-0011200, Slide 7. This type of manufacturer authorization would need to be adjusted to comply with the RTR Law if the J-1962 connector is the method used to comply with Section 3 of the law.

166. To maintain an authorization system for access to vehicle networks and their on-board diagnostic systems, OEMs will need to ensure there is a standardized third-party method on which to authorize their tool as a diagnostic tool that is permitted to make all necessary diagnostic repairs, potentially by managing the certificate approvals for tool manufacturers.

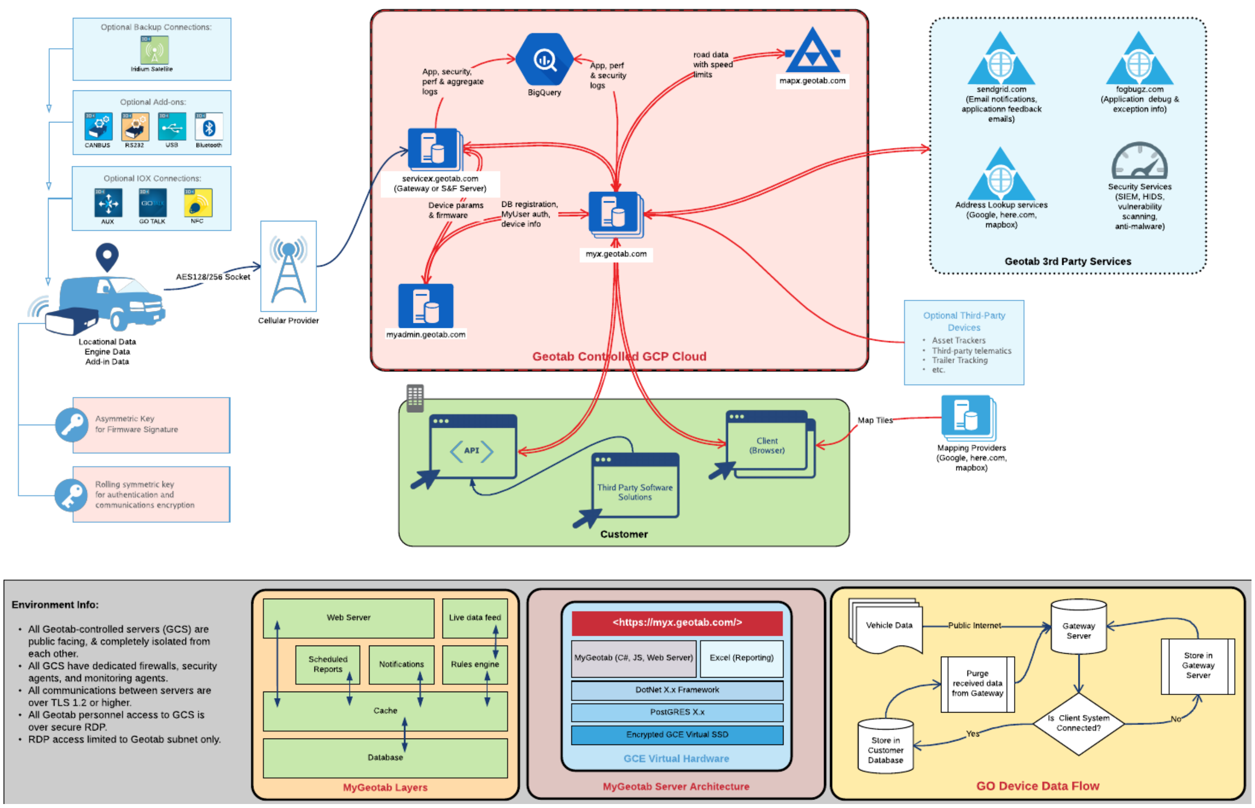
167. Currently, ETI acts as a third party that administers authorization/vetting for third-party diagnostic scan tool companies. ETI and the OEMs have an existing relationship, and ETI is one potential unaffiliated entity that could provide standardized authorization of repair tools.

168. Another alternative could be the NASTF SDRM program. NASTF is an independent organization that was set up to facilitate cooperation between the OEMs and aftermarket that handles things such as authorizing replacement keys for locksmiths. The SDRM program verifies the business, checks insurance, and performs background checks to validate the vehicle owner or business. Encryption keys are similar to the physical keys that the NASTF SDRM program already handles. Whereas physical keys provide access to the vehicle and enable driving it, cryptographic keys provide access to diagnostic and repair functionalities. The auto industry already trusts NASTF for physical security validation of their vehicles. If the NASTF SDRM program was expanded to issue encryption keys on behalf of the OEM after validating a vehicle owner or tool manufacturer, it could be a viable unaffiliated entity.

169. Telematic dongles would require a significantly mature security posture to support certificates. Cheap dongles would still be prevented from performing diagnostic actions unless they could support certificate storage, such as key-signing, encryption, and

requesting the issuance of a certificate from a third party. The ability to support such technologies demonstrates an above-average security posture and provides an adequate bar of entry for performing basic telematic tasks.

170. The image below outlines how a mature telematics provider, GeoTab, provides fleet management services. Telematic dongles can encrypt traffic back to their backend servers over standard HTTPS (the same encryption web browsers use) or other encrypted tunnels. Bi-direction commands can be issued from a mobile application, through the telematic provider's servers and into the consumer's vehicle to perform the same tasks provided by the OEMs.



171. In addition, it's possible that the OEMs could use multiple telematic dongle vendors whose authorization system is run by an unaffiliated entity. Having multiple vendors is

like having multiple scan tool companies; they all have a standard way to communicate, but if one scan tool has a vulnerability, they will not all be affected. If consumers have options to choose different telematic providers, then a security vulnerability would only affect one brand, reducing the amount of vehicles affected. When only the OEM provides telematics, you have a single point of failure. A security vulnerability with the OEM provider would affect every vehicle in their fleet. By enabling multiple telematic dongle vendors, the risk of a vulnerability would be distributed, which enhances vehicle security. If a telematics dongle provider had a vulnerability, the authorization certificate for that provider could be revoked by the unaffiliated entity administering the authorization system until the vendor has corrected the vulnerability.

172. A public key infrastructure authorization system that is standardized across all makes and models in the Commonwealth could be developed and made fully operational in six months. To develop the authorization system the OEMs would need to select the unaffiliated entity to serve as the certificate authority and agree to an application programming interface (API) as a standard way of communicating.

b. <u>Developing a Fully-Telematic Platform to Support Remote Diagnostics in Compliance With the RTR Law</u>

173. The OEMs could alternatively design an inter-operable, standardized and open access telematic platform that is capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection and can be directly accessed through a mobile-based application, including the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair.

174. A telematic platform could consist of an independent module/ECU or wireless capabilities embedded into an In Vehicle Infotainment (IVI) system or other module.

175. But, wherever it is located on the vehicle, because of its wireless nature, it is important that a telematic platform employs additional security that is not present in a J-1962 (OBD) connector. The telematic platform should be segmented and isolated from the majority of the vehicle. Because telematic devices and IVI systems have a larger attack surface than the average ECU by including wireless communications, special care needs to be taken to ensure an unauthorized third party cannot attack the system.

176. Protection strategies for systems with a high attack surface can and should involve layering multiple controls and mitigating factors to reduce risk of compromise or damage. For a telematic platform, core controls would likely involve segmentation/isolation, authentication/authorization, and privacy/encryption.

177. In addition, a telematic platform could utilize wireless communications in the spectrum of Bluetooth, WiFi or Cellular communications. Each of these technologies provides different levels of range and capabilities, but any of these technologies could be used in order to be compliant with the RTR Law.

178. It is important that wireless communication uses authentication and encryption. You can further limit the range that an attacker can use by selecting the type of wireless communication. Both Bluetooth and Wifi imply a near field communication, less than 300 yards, and cellular implies global communications. Bluetooth and Wifi traditionally only operate on a single connection, meaning that you must authenticate to the vehicle in order to access the Bluetooth or WiFi connection. Cellular connections can be used to operate an entire fleet and while often recommended, it does not inherently imply authentication.

All three wireless technologies deploy different methods of encryption and it is encouraged that each one use the latest security standards when configuring their encrypted connection.

179. Segmentation consists of putting specific ECUs on their own bus line to separate them from the rest of the vehicle's network. These segmentations can be done to preserve bandwidth use, insulate safety critical systems, and/or isolate high risk ECUs. [redacted] Deposition of Kevin Baltes, 4.15.21, pp. 214-15.

180. The term isolation is more general and can also consist of separating functionality within an ECU. Processes, memory and other functionality can all be isolated internally within an ECU or IVI module. In the case where the telematic functionality is built into a more complex system such as an IVI, the telematic portions can be further isolated to ensure that a compromised telematic device does not jeopardize the functionality of the rest of the ECU. Isolation can be achieved by things like a hypervisor to isolate, physical separation of different chips and sandboxing, [redacted]. Deposition of Kevin Baltes, 4.15.21, pp. 109-11 and 171-73.

181. Authentication represents confirmation of the identity of an individual, a company, or other actor. In the case of this discussion this would represent the vehicle owner, repair shop or tool manufacturer.

182. Authorization represents the actor's role or what it can do on a system. Much like a job function, an authorization is what allows you to perform a certain action.

183. It is important to draw a distinction between authentication and authorization for purposes of the RTR law, because Section 2 of the law only requires manufacturer authorization to a vehicle's on-board diagnostic system to be administered by an unaffiliated entity. Using a telematic platform to comply with Section 3 of the RTR law, Section 2 of the law is not directly implicated. Nevertheless, if a manufacturer develops a telematic platform to comply with Section 3, that telematic system must be open access. If an OEM uses a Public Key Infrastructure (PKI) to provide security to the telematic platform, then that PKI must be administered by a third party in order to be open access. If a manufacturer served as its own certificate authority, then the direct access to the platform necessary for diagnostics, maintenance, and repair would be gated by the OEM rather than open access.

184. For traditional diagnostics using UDS, it is possible to use Mode 27 (SecurityAccess) to provide authorization. *Security Access Service Identifier (0x27): UDS* Protocol, PiEmbSysTech Embedded Research Blog, https://piembsystech.com/security-access-service-identifier-0x27-uds-protocol/. This is done with a seed-key algorithm, which is a challenge. The ECU provides a number and if you return the expected response number that the ECU was expecting then it unlocks the requested diagnostic functions. Traditionally there is no check as to who is performing this action, as long as the response is correct then access is allowed. This is very similar to a password system that does not require a username.

185. For more advanced encryption such as those used in PKI, a certificate is used to authenticate an action. PKI systems use public and private keys to verify identity. For a telematic diagnostics platform, the receiving telematic system would need to check the

incoming connection to determine the intention of the request and to confirm that the requester is allowed to make that request. The telematics system would check the certificate to verify the request is coming from a valid source and has been provisioned for the action it is trying to take.

186. Certificate based solutions ensure that a connection or an update is created by a trusted or valid source. These certificates can also embed additional data that can be used to define a role, issue time, expiration, and any other useful data needed to perform validation. [redacted] in Exhibit 9: AAI-FCA-0011200:

[redacted]

In a fully-telematic "remote diagnostics" platform, authentication could be implemented in different ways. If the connection is local over Bluetooth or WiFi, then the connection can be authenticated by the typical Bluetooth or Wireless authentication mechanisms already built into those wireless protocols. For instance, when you pair a Bluetooth device the Infotainment screen will show a number that should match what you see on your screen. But if the connection is over Cellular, then the OEM could use a third party to authenticate the requester. The third party could operate like NASTF, which is used by OEMs and locksmiths. NASTF validates the locksmith or vehicle owners and can issue keys on behalf of the OEMs.

187. Authorization could be employed in a telematic platform by the same methods that is used via the J-1962 connector. Once a connection has been authenticated an OEM could rely on existing authorization mechanisms. If an OEM is using a PKI certificate based system, it can embed the approved role into the certificate that is passed to the vehicle. Based on the testimony of GM's Kevin Baltes, diagnostics are filtered by the gateway using an identifier. Deposition of Kevin Baltes, 4.15.21, p. 214. This security could be improved by using the certificate from the telematics passing to the gateway to enable diagnostics for just that session.

188. It should be noted that there are many ways to solve these problems and different OEMs have different architectures. Although not all OEMs use gateways to filter traffic, adding filtering gateways or other security measures adds additional mitigation controls, producing a defense-in-depth approach.

189. Another important piece of wireless communications is to ensure transmitted data is protected from eavesdroppers. Eavesdropping attacks, also referred to as man-in-the-middle attacks by security professionals, are initiated by attackers to gather the content of sensitive communications and/or alter a network communication in transit. A secure wireless system will typically deploy encryption and signing to combat these categories of attacks.

190. Both Bluetooth and WiFi use encryption as an industry standard to protect wireless communications. Most cellular communication also utilizes encryption, and may also use Transport Layer Security (TLS) or a Virtual Private Network (VPN) to further protect the communication. GM's Kevin Baltes testified that GM requires use of TLS 1.2 for the vehicle ECUs that are capable of connection to cellular. The recommendations for cellular

match the same industry standard recommendations as a standard internet connection, since a cellular connection operates in relatively the same manner as a standard internet connection. Both TLS and VPN solutions can also be used for WiFi communication for additional protection.

i. <u>Implementation</u>

191. In the case of GM and FCA, they would not need to build out a new hardware telematic solution in order to be compliant, [redacted] They would need to develop, test, and deploy a new version of firmware (embedded software) to upgrade the existing telematics systems.

192. In a fully telematic diagnostic platform, diagnostic communications would happen in the same manner that they happen via the J-1962 (OBD) connector. Communication to the target ECU for diagnostics would simply have to route back to the telematics unit instead of the J-1962 connector when communications initiate from the telematic module. An OEM could accomplish this by ensuring that the telematic platform can communicate to the ECU in question. Under normal circumstances, the OEM would not have to perform any additional actions to achieve this communication.

193. If there is a gateway with filtering capabilities that controls packets between network buses, then it may need additional rules to permit the telematics to perform diagnostic functions. The gateway will need to be configured to also manage diagnostic

packets originating from the telematics in the same manner that they originate from the J-1962 connector.

194. In Kevin Baltes' deposition he states that [redacted] Deposition of Kevin Baltes, 4.15.21, pp. 214-15. The gateway could further be configured to require a certificate that validates a role before it enables communications. Using a central gateway to filter diagnostic requests sent telematically would provide an additional layer of security. By filtering the messages sent telematically to the vehicle, the central gateway module will be able to block unsafe requests or commands sent by hackers. The central gateway, which OEMs like GM already use, would prevent unapproved and dangerous commands from even reaching the ECUs, which are the components that would need to be reached to affect vehicle functions. All rationality checks to ensure safety is taken into consideration would still apply.

195. Diagnostic communications via the OBD connector typically occur via UDS over the CAN bus, which operates at 500k bus speeds. Bluetooth, WiFi and Cellular can all handle these speeds – Bluetooth is the slowest of the three, with a maximum speed of 1000k. If, however, a vehicle's bus speed is faster than CAN, such as CAN-FD which has a top speed of 12M, WiFi and Cellular remain wireless options.

196. Encryption does not need to happen on the bus or the internal vehicle network but it should happen once the diagnostic packets are transmitted over the selected wireless communication protocol (Bluetooth, WiFI, Cellular), as described above.

197. Making the telematic platform "open access" does not mean that it could not have safety and security controls. "Open access" simply means that the OEM doesn't control access to the platform.

198. If the telematic platform uses Bluetooth or Wifi to create a direct connection with the mobile device, and the telematic system can connect through the gateway without the need to authenticate via a PKI certificate system, then that platform would be open access to the user. But, if the telematic system uses a cellular connection, then the OEM will need to utilize a TLS encrypted communication. Even if the mobile device is physically local to the vehicle, both the telematic platform and the mobile device will connect to the internet via cellular and will require encryption to connect. If the OEM has set up a private PKI system to control authentication and or authorization, then in order to be considered "open" they would need to use a third party as their certificate authority. This operator could be set up in a similar manner as NASTF.

199. A telematics platform would be inter-operable if it follows the same methods as the J-1962 over Bluetooth, WiFi, or cellular. The additional access requirements such as certifications should come from an unaffiliated third party to validate and authorize the user or device. Once the connection is secured and authorized then all diagnostics can be performed in the same manner as the non-wired equivalent of the tool.

200. The RTR Law requires the platform to be "standardized" across all of an OEM's makes and models, which means that the platform must follow a well-documented method to perform actions such that there is a common way of communicating. The SVI standards, addressed in greater detail in Brian Romansky's expert report, could be applied to a fully-telematic platform to achieve standardization.

201. The RTR Law also requires the platform to be directly accessible by users. If the telematic platform uses Bluetooth or WiFI, then the diagnostic tool can be done via a phone application. The phone can proxy the request to the third party provider, validate

ownership or right to perform maintenance and then pass this information to the telematic device. Once the telematic device receives this information it then internal validates or passes this information to the central gateway to validate. Once validated the requested diagnostic capabilities are enabled for that session and the phone application can be used to perform the diagnostic or repairs.

202. In the case of a cellular solution, the communication would need to route over the internet. The vehicle's cellular network would connect to a backend system. This backend system could be the OEMs backend or a third party backend. Data that is normally sent to the OEMs backend systems should be sent to the third party or made available to the third party in order to provide the same predictive maintenance solution and reminders that the OEM and dealership can provide. The customer or repair shop would use their phone or a separate tool to communicate with the third-party system to authenticate and authorize maintenance. The network communications from the customer's device to the vehicle would route through the internet and would need additional encryption, either TLS or VPN technology can be used to secure this communication.

203. The RTR Law requires access to mechanical data to include the ability to send commands to in-vehicle components if necessary for diagnosis, maintenance, or repair. To provide this access, the telematic platform the OEMs develop to comply with the RTR law would need to route all diagnostic-related commands through the telematic platform. The OEM typically would not have to do anything additional to allow the telematic system to perform diagnostic functions as any device on a network can typically communicate to other devices. If the OEM has specifically filtered the telematic system using a gateway, then they would need to modify the filtering rules via a configuration change.

204. Without information about how an individual OEM has filtered the telematic system using a gateway, I cannot provide more specifics about what modifications would need to be made to the filtering rules. If the OEMs had provided consistent and up-to-date documentation on how their gateway worked, or allowed me to use the same tools they use to analyze the .arxml files they produced so that I could gain insight into their policies for configuration changes, I would have been able to provide more specifics. The OEMs can easily determine how to modify the filtering rules via a configuration change, because they have access to their existing policies for making this type of configuration change.

205. It is possible to construct a telematics platform that would still ensure vehicle safety while being capable of accepting commands necessary for diagnosis, maintenance, or repair. When diagnostic commands come in via a secure telematic connection it can then be validated . After validation diagnostic commands will then be able to route to and from the remote connection to the ECU being diagnosed, providing the vehicle is in a safe state to perform the diagnostic operations and ECUs' rationality checks are met. These checks occur regardless if the diagnostic request comes in over the J-1962 connection or over telematics.

206. Authentication and authorization still needs to be addressed by all the OEMs regardless of where the platform is located in the architecture. In order to be open and accessible, a third-party system will need to stand up to proxy authentication requests on behalf of the OEMs. This organization can be similar or even utilize existing collaboration with other third party groups such as ETI or NASTF. The third party group would validate vehicle owners, tool manufacturers and repair shops providing authentication. They would

then relay the response for seed-key or encryption certificate for the vehicle and maintenance requested providing authorization.

ii. Development Time

207. Creation of a fully telematic platform will require time to design, test, and validate. But the amount of time will vary depending on the specific OEM and the specific model vehicle.

208. For OEMs such as GM and FCA that already use, in at least some of their vehicles, hardware architecture that includes many of the features appropriate for a fully telematic platform, development time may be limited to the time necessary to prepare and distribute necessary Over-The-Air (OTA) software updates.

209. For OEMs and vehicles that do not already have proper segmented vehicle architectures, gateways, encryption capabilities, or other features required for a secure telematic platform, the time to design, test, and validate the necessary architectural changes would probably be one to two years.

210. Vehicles with telematics systems, which are the only ones subject to Section 3 of the RTR Law, are the ones most likely to already have the features required for a secure telematic platform.

VI. Conclusion

211. An OEM could feasibly and securely comply with Section 3 of the RTR Law immediately by disabling the telematics systems of vehicles it sells in Massachusetts.

212. An OEM could feasibly and securely comply with Section 3 of the RTR Law by using any platform that meets the requirements of Section 3. In the medium-term, one possible platform could be the existing J-1962 connector combined with a plug-in telematic

"dongle." In the longer term, OEMs could adjust the vehicle network architectures on new vehicles to comply with the law by using a fully telematic platform. OEMs can take as much time as needed to implement the fully-telematic platform by using the J-1962 and telematic dongle in the interim.

213. By utilizing an unaffiliated entity for a standardized authorization system for the telematics dongle, a neutral method to distribute a secure platform that protects against external hackers can be achieved.

214. Furthermore, most API and certificate methodologies demonstrated by the OEMs are easily extendable to support additional third party certificate services such as those I recommend. OEMs have the ability to comply with the RTR Law without creating security risks to their vehicles.

I declare under the penalty of perjury that the foregoing is true and accurate, this 26 day of May 2021.

Craig Smith

Exhibit 519

2715B W. Jameon St
Seattle, WA 98199
(513) 275-1989
agent.craig@gmail.com

Craig Smith

SKILLS

Experienced leader in security research, with a demonstrated history of working in the product and information security sectors. With both a strong technical background and a thought leader for emerging technology sectors. Strong background in information security, exploit development, reverse engineering, threat modeling, policy development, standards bodies and most recently transportation related security. Often working directly with standard organizations such as SAE, ISO, IEEE and W3C as well as government groups. With many presentations and keynotes and industry and security conferences as well as several major media outlets. Author of the Car Hacker's Handbook, many open source tools and frameworks and the founder of both Open Garages and Hive13 Hackerspace. Government Clearance.

EXPERIENCE

Bird, LA, CA — *Senior Director of Security*

July 2019 - PRESENT

- Led Bird's Information security teams and oversaw Infrasec, application security, product security and physical security (GSOC)
- Built out an international security program that went from factory development to tracking a full set of KPIs for executive and board members
- Developed KPIs and gave regular updates to the rest of the exec team and board members
- Reduced security opex spend by over 3 million dollars while still maintaining an equivalent level of security.
- Developed an effective plan for health and safety during the COVID-19 pandemic as well as worked to reduce direct law enforcement engagements for non-violent offenses.

Byton, Senior Santa Clara, CA — *Senior Director of Product Security*

October 2018 - June 2019

- Led Byton's Information security teams, incident response, vulnerability management, investigations, threat hunting, awareness and training, divisional budget management and leadership.
- Worked directly with investors and outside stakeholders.

- Managed custom hardware and firmware products from a production timeline as well as security perspective.

Rapid7, Boston, MA — *Director of Transportation Security*

August 2016 - October 2018

- Research included planes, trains, automobiles, maritime, and anything else that moved.
- Specialized in the hardware components that make up transportation technologies.
- Focused on working with engineers to build hardware that is capable of dealing with complex software updates as well as environments were multiple stakeholders need to make changes to the firmware.
- Performed threat modeling, device security assessments, penetration testing as well as deploying analysis systems that can work on more than just Ethernet.

Theia Labs, Seattle, WA — *Owner*

January 2011 - August 2018

- Technology research, specializing in reverse engineering of software and hardware protections, mobile devices and augmented reality research.
- Developed new and innovative tools and technologies for corporations and we have clearance for government research.
- Provided subcontracting and support for other security focused organizations.
- Developed heuristic analysis engines for android devices and custom Dalvic debuggers.
- Performed several automotive related security audits as well as create custom CANBus sniffers for team analysis.

PUBLICATIONS

The Car Hacker's Handbook

March 2016 - No Starch Press

The Car Hacker's Handbook will give you a deeper understanding of the computer systems and embedded software in modern vehicles. It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and between devices and systems.

Then, once you have an understanding of a vehicle's communication network, you'll learn how to intercept data and perform specific hacks to track vehicles, unlock doors, glitch engines, flood communication, and more. With a focus on low-cost, open source hacking tools such as Metasploit, Wireshark, Kayak, can-utils, and ChipWhisperer.

The Car Hacking Village - Co Founder

2014 - Present - Defcon, Las Vegas

The primary goal of the Car Hacking Village is to build a community around discovering weaknesses and exposing vulnerabilities that could significantly impact the safety and security of all drivers and passengers on the road today. Educating security researchers on the functionality of vehicle systems coupled

with providing them with the opportunity to gain hands-on experience working side by side with experts in this field is a plus for the attendees. Leveraging the vast amount of experience the security research community brings to the Village may increase the safety and security of vehicles on the road today and for generations to come.

AWARDS

Spoke at many of the worlds hacker and industry conferences as a keynote speaker.

Trusted advisor and reviewer for SAE and IEEE.

Over a dozen technical certifications.

Exhibit 515

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION, Plaintiff, v. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEWALTH OF MASSACHUSETTS in her official capacity, Defendant.	CIVIL ACTION NO. 1:20-cv-12090-DPW

PLAINTIFF ALLIANCE FOR AUTOMOTIVE INNOVATION'S FIRST SUPPLEMENTAL RESPONSES TO ATTORNEY GENERAL MAURA HEALEY'S FIRST SET OF INTERROGATORIES

PORTIONS OF RESPONSE 5 CONFIDENTIAL

Pursuant to Rules 26 and 33 of the Federal Rules of Civil Procedure, Plaintiff Alliance for Automotive Innovation ("Auto Innovators"), by and through its undersigned counsel, hereby supplements its February 23, 2021 Responses to Attorney General Maura Healey's ("Defendant") First Set of Interrogatories (the "Original Responses") as follows:

PRELIMINARY STATEMENT

Auto Innovators' responses to the Defendant's First Set of Interrogatories (the "Interrogatories," and each individual interrogatory contained therein, an "Interrogatory") are made solely for the purpose of this action. Each response is made subject to all objections as to competence, relevance, materiality, propriety, admissibility, and the like, and any and all other objections on grounds that would require the exclusion of any response herein if such were offered in Court, all of which objections and grounds are reserved and may be interposed at any time, including at the time of trial. Auto Innovators' responses are not intended to be, and shall not be construed as, a waiver by Auto Innovators of any or all objections to the Interrogatories. Auto Innovators' objection or response to any Interrogatory should not be taken as an admission that Auto Innovators accepts or admits the existence of any fact(s) or any information assumed by that Interrogatory or that such objection or response constitutes admissible evidence.

Certain of the information requested in the Interrogatories is within the unique knowledge of persons and entities other than Auto Innovators. Nevertheless, as discussed at the December 18, 2020 status conference, where appropriate, Auto Innovators is providing information requested in the Interrogatories that relates specifically to the members designated to provide fact witnesses at trial, namely FCA US LLC ("FCA"), General Motors LLC ("GM"), Mercedes-Benz USA LLC ("MBUSA"), and Toyota Motor North America Inc. ("TMNA") (collectively, the "Designated Members").[1]

[1] Though Auto Innovators adopts this portion of Defendant's terminology, it does so subject to its objections below.

Neither Auto Innovators nor the Designated Members have completed their (a) investigation of the facts relating to this case, (b) discovery in this action, or (c) preparation for trial, and Auto Innovators reserves the right to supplement these responses as may be appropriate. The following responses are based upon information known at this time to Auto Innovators and are given without prejudice to Auto Innovators' right to amend, supplement or revise these responses with any subsequently discovered information.

GENERAL OBJECTIONS

Auto Innovators makes and hereby incorporates by reference the following general objections, whether or not separately set forth, in response to each Interrogatory:

1. Auto Innovators objects to each Interrogatory to the extent it seeks information that is subject to the attorney-client privilege or the work product doctrine or that is otherwise privileged or protected pursuant to any applicable doctrine, statute, or rule. Such responses as may hereafter be given shall not include any information protected by such privileges, doctrines, statutes or rules, and inadvertent disclosure of such information shall not be deemed a waiver of any such privilege or protection.

2. Auto Innovators objects to each Interrogatory as overbroad and unduly burdensome, including to the extent it seeks information that is more readily or equally available to Defendant from other sources for whom it is more convenient, less burdensome, or less expensive to produce the requested information, or to the extent that the information requested in these Interrogatories has been provided to Defendant through other means, including in the documents produced by Auto Innovators and the testimony of its witnesses.

3. Auto Innovators objects to each Interrogatory that fails to specify a relevant time period for the information requested, and to the extent any Interrogatory seeks information for an unlimited time period, such Interrogatory is overbroad and unduly burdensome. Auto Innovators further objects to each Interrogatory that requests information "from 2015 to the present" as overbroad, unduly burdensome, and seeking information that is irrelevant because it is outside

the scope of issues in this case. Unless otherwise stated, Auto Innovators provides information for the time period from January 1, 2018 to the present.

4. Auto Innovators objects to each Interrogatory and to the Definitions utilized in those Interrogatories to the extent they assume facts not in evidence. By responding and objecting to each of these Interrogatories, Auto Innovators does not admit or agree with any explicit or implicit assumptions made in these Interrogatories or the Definitions utilized therein.

5. The Interrogatories seek information that is private, proprietary, trade secret, confidential business, or personal information. Auto Innovators will produce any such information only pursuant to the protections of the Confidentiality Protective Order in this case and/or applicable provisions of the Federal Rules of Civil Procedure.

6. Auto Innovators objects to each Interrogatory to the extent it seeks information not within Auto Innovators' possession, custody or control.

7. Auto Innovators objects to each Interrogatory to the extent it purports to impose any obligations not imposed by the Federal Rules of Civil Procedure, the Federal Rules of Evidence, the Local Rules of the U.S. District Court for the District of Massachusetts, the Court's standing orders, the Scheduling Order and Confidentiality Protective Order in this case, and any other applicable rules or law. Auto Innovators will respond to these Interrogatories in accordance with its obligations under applicable rules and law.

8. Auto Innovators objects to the definition of "To 'Identify' (when referring to a device, element of design, Telematics System, On-Board Diagnostic System, or other thing)" on the basis that such definition is overbroad and unduly burdensome, it is vague and ambiguous, and it renders certain Interrogatories duplicative of one another.

9. Auto Innovators objects to the definition of "You" to the extent it requires the provision of information not in the possession, custody, or control of Auto Innovators. Auto Innovators will only provide information, including information predating the merger of the Association of Global Automakers and the Alliance of Automobile Manufacturers, that is in Auto Innovators' possession, custody, or control. Further, Auto Innovators responds only on

behalf of itself, and not on behalf of its officers, directors, employees, partners, corporate parents, subsidiaries, or affiliates.

10. Auto Innovators objects to the definition of "Designated Member" to the extent it purports to require the provision of information by persons other than FCA, GM, MBUSA, and TMNA, including but not limited to officers, directors, employees, partners, corporate parents, subsidiaries, or affiliates of those entities.

11. Auto Innovators objects to the definitions of "Actively Participating Member" and "Other Member" and to Instruction no. 1 to the extent they purport to require collection and provision of information related to entities other than FCA, GM, MBUSA, or TMNA that is not already in the possession, custody, or control of Auto Innovators. At the December 18, 2020 conference, the Court instructed that discovery would be available from Auto Innovators and the "five or so . . . association representatives who would be deposed." Dec. 18, 2020 Tr. at 5:2-25. The Court further stated that "no more than five companies and their representatives is sufficient to . . . give you the opportunity to learn about and develop the questions of what their proprietary information is." *Id.* at 17:3-7. Where appropriate to respond to these Interrogatories, and except as otherwise provided herein, Auto Innovators only provides information from FCA, GM, MBUSA, and TMNA, which are the four Auto Innovators members who will provide fact witness testimony. In addition, the information provided from the Designated Members will be limited to the scope of the testimony they agreed to provide, as described in Auto Innovators' Initial Disclosures.

12. Auto Innovators objects to the definition of "Telematics System" as vague and ambiguous, including because many motor vehicle telematics systems do not "collect" information generated by vehicle operation and because the functionality of telematics systems varies significantly.

13. Auto Innovators objects to the various Interrogatories below which are compound, conjunctive, subjunctive, and/or contain subparts, as described in response to each Interrogatory below. In addition, Defendant has inadvertently labeled two separate

Interrogatories with the same number (18). Auto Innovators reserves all rights to object to Defendant propounding additional Interrogatories that exceed the maximum permitted by Rule 33 of the Federal Rules of Civil Procedure and/or the Local Rules of the U.S. District Court for the District of Massachusetts.

14. Auto Innovators' responses reflect only the current state of its knowledge or information regarding the information Defendant has requested. Further investigation may identify additional facts or information that could lead to additions to, changes in, and/or variations from, the responses herein. Without in any way obligating itself to do so, Auto Innovators expressly reserves the right to supplement, amend, correct, clarify or modify the responses as further information becomes available.

SUPPLEMENTAL RESPONSES TO INTERROGATORIES

Subject to the above Preliminary Statement and General Objections, which are incorporated into each specific objection and response below, Auto Innovators further objects and responds to the Interrogatories as follows:

INTERROGATORY NO. 4

For each type of vehicle Identified in response to Interrogatory No. 2 or Interrogatory No. 3:

a. State whether some, all, or none of the individual vehicles of that type are or will be equipped with a Telematics System when sold;
b. Identify each Telematics System with which an individual vehicle of that type is or will be equipped when sold;
c. Identify each On-Board Diagnostic System with which an individual vehicle of that type is or will be equipped when sold.

RESPONSE TO INTERROGATORY NO. 4

Auto Innovators specifically incorporates by reference the above Preliminary Statement and General Objections as if fully set forth herein. Auto Innovators further incorporates by reference its objections to Interrogatories nos. 2 and 3, which are referenced in this Interrogatory.

Auto Innovators further objects to this Interrogatory and definition of "Identify" as used herein because they are overbroad, unduly burdensome, not proportional to the needs of the case, and call for irrelevant information. Auto Innovators further objects to this Interrogatory and the definition of "Telematics System" for the reasons stated in paragraph 12 of the General Objections above. The identification of which telematics and/or on-board diagnostics systems are present on which make, model, model year, and trimline of every type of vehicle sold or planned to be sold by any member of Auto Innovators over a five-year period in the entire Commonwealth of Massachusetts—together with the part, version, and model numbers of those systems and the identification of all persons with knowledge about those systems—would be an extremely burdensome exercise yielding little, if any, information relevant to this case. Auto Innovators further objects to this Interrogatory as compound, conjunctive, and disjunctive, and as containing subparts. Auto Innovators further objects to this Interrogatory as vague and ambiguous, as "On-Board Diagnostic System" is undefined and, to the knowledge of Auto Innovators, vehicles' on-board diagnostics functions are fully integrated into vehicle controls and do not constitute a separate unit. Auto Innovators further objects to this Interrogatory as overbroad as to time; Auto Innovators will only provide information related to model years 2018 to the present, as well as known information related to future model years through model year 2025. Auto Innovators further objects to this Interrogatory to the extent the information in this Interrogatory may be provided to Defendant through other means, including in documents produced by Auto Innovators. Auto Innovators further objects to the extent it seeks information from the Designated Members beyond that designated in Auto Innovators' Initial Disclosures. Subject to and without waiving said objections, Auto Innovators responds as follows:

GM

Though Auto Innovators rests on its time-frame objection, it states that beginning with model year 2015, with the exception of certain motor vehicles sold outside typical consumer channels (*e.g.*, sales to fleet vehicles and incomplete trucks), all motor vehicles sold by GM come equipped with GM's telematics system, which is called On-Star. Information related to

diagnosis, maintenance, and repair is only a subset of the information transmitted through On-Star, and GM's responses to these Interrogatories are limited to On-Star's functionality with respect to that information. GM vehicles have included some version of the On-Star system for over a decade. The On-Star telematics system on GM motor vehicles can be deactivated at any time by customers, including at the time of sale. Current model year vehicles use the eleventh generation of On-Star, but GM plans to implement the twelfth generation of On-Star in the near future; its exact timing for doing so is not known and will vary by make and model.

All emissions-certified GM motor vehicles are equipped with On-Board Diagnostic systems, as is required by state and federal regulations, and those systems conform to SAE J1979, as incorporated by reference in the aforementioned regulations. Those OBD systems are not branded, and they are not separate modules but are embedded in the controls of motor vehicles.

FCA

Though Auto Innovators rests on its time-frame objection, it further states that many FCA motor vehicle models have had standard or optional telematics systems (i.e., VP4, VP4R, or TBM, as described below) since model year 2013. Most FCA motor vehicle models from model year 2018 onward include such systems. Alfa Romeo Giulia and Alfa Romeo Stelvio vehicles had such telematics systems from model years 2020 onward; Ram Promaster vehicles had such telematics systems from model year 2022 onward; and Alfa Romeo (4C), Ram Promaster City, Dodge Journey, Dodge Caravan, Dodge Dart, and Fiat models do not have such telematics systems. The telematics systems are as follows:

- <u>Value Proposition 4 (VP4)</u>: FCA's "first generation" telematics system, which was optional in certain vehicles between model year 2013 and model year 2018. This telematics system was manufactured by Harmon and uses a Sprint cellular connection. The VP4 system is embedded within the vehicle's touchscreen radio.
- <u>Value Proposition 4R (VP4R)</u>: FCA's "second generation" telematics system, which was optional on certain vehicles between model year 2017 and model year 2021. This

telematics system was manufactured by Panasonic and uses an AT&T cellular connection. The VP4R system is embedded within the vehicle's touchscreen radio.

- Telematics Box Module (TBM): FCA's "third generation" telematics system, which has been optional on some vehicles and standard on other vehicles beginning in model year 2020. This telematics system has separate hardware that connects directly to FCA.
- Fleet Telematics Module (FTM): Some FCA vehicles (including certain Ram trucks and fleet vehicles) may have a standalone telematics device called FTM, which is sold through Verizon.

All FCA motor vehicles are equipped with On-Board Diagnostic systems. The OBD systems are not branded, and OBD is not a separate module but is embedded in the controls of the car and distributed among all vehicle electronic control modules.

MBUSA

Though Auto Innovators rests on its time-frame objection, it further states that for the model year 2018 onward, all motor vehicle models distributed by MBUSA, except for "smart" brand models, have had telematics systems. Mercedes-Benz vehicles may contain one of two types of telematics systems: mbrace®, which existed on various Mercedes-Benz models in model year 2018, and Mercedes me connect (Mmc), which has existed on various Mercedes-Benz models in model years 2018 to 2021. For model year 2018, most Mercedes-Benz models used mbrace® systems, though some C-class vehicles and GLE-class vehicles used Mmc systems. For model years 2019-2021, all Mercedes-Benz models with telematics systems used Mmc.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 4

Subject to and without waiving the above objections, Auto Innovators supplements its response as follows:

TMNA

Though TMNA rests on its time-frame objection, it further states that for the model year 2018 onward, some Toyota and Lexus models have had a telematics product called "Service Connect" that transmits vehicle diagnostic information. Service Connect has been present in certain Lexus vehicles from model year 2015 onward. Service Connect has been present in certain Lexus ES 300H, ES 350, GX 460, IS 300, LC 500, LC 500H, NX 300, NX 300H, RC 300, RC 350, RC F, RX 350, RX 350L, RX 450H, and RX 450HL models between model year 2018 and the present; certain Lexus UX 200 and UX 250H models between model year 2019 and the present; certain Lexus IS 350, LS 500, and LS 500H models between model year 2020 and the present; and certain Lexus ES 250 and IS 200 models in model year 2021. Service Connect has been present in certain Toyota Camry models since model year 2018; in certain Toyota Avalon, Corolla hatchback, and RAV4 models since model year 2019; in certain Toyota Corolla sedan, 4Runner, Highlander, Sequoia, Tacoma, and Tundra models since model year 2020; and in certain Toyota Mirai, RAV4 Prime, Prius Prime, Sienna, and Venza models since model year 2021. Service Connect currently is not available in any Toyota C-HR, Prius, or Prius Prime models.

INTERROGATORY NO. 5

For each Telematics System Identified in response to Interrogatory No. 4:

a. State whether the wireless transmission function of that Telematics System is capable of being disabled and, if so, how, by whom and under what conditions;

b. State all categories of information "used for or otherwise related to the diagnosis, repair or maintenance of the vehicle" that are, or will be, collected by that Telematics System; and

c. Identify all Persons with knowledge Concerning the ways in which information collected by that Telematics System is, or will be, made accessible to vehicle owners or independent mechanics.

RESPONSE TO INTERROGATORY NO. 5

Auto Innovators specifically incorporates by reference the above Preliminary Statement and General Objections as if fully set forth herein. Auto Innovators further incorporates by reference its objections to Interrogatory no. 4, which are referenced in this Interrogatory, as well as its objections to Interrogatories nos. 2 and 3, which are referenced in Interrogatory no. 4. Auto Innovators further objects to this Interrogatory and the definition of "Telematics System" for the reasons stated in paragraph 12 of the General Objections above. Auto Innovators further objects to this Interrogatory as overbroad, unduly burdensome, ambiguous, and vague because it requests "all" categories of information that are "used for or otherwise related to the diagnosis, repair or maintenance of the vehicle"—which would appear to include most data generated, stored in, or transmitted by a motor vehicle. Auto Innovators further objects to this Interrogatory as overbroad and unduly burdensome because it requests "all Persons" with knowledge concerning information from telematics systems that would be made accessible to vehicle owners of independent mechanics—which apparently would include thousands of individuals. Auto Innovators further objects to this Interrogatory as overbroad as to time; Auto Innovators will only provide information related to model years 2018 to the present, as well as known information related to future model years through model year 2025. Auto Innovators further objects to this Interrogatory as compound, conjunctive, and disjunctive, and as containing subparts. Auto Innovators further objects to this Interrogatory to the extent the information in this Interrogatory may be provided to Defendant through other means, including in documents produced by Auto Innovators. Auto Innovators further objects to the extent it seeks information from the Designated Members beyond that designated in Auto Innovators' Initial Disclosures. Subject to and without waiving said objections, Auto Innovators responds as follows:

GM

OnStar's wireless transmission function is capable of being disabled. It can be disabled by an On-Star representative, through an over-the-air signal, if the GM motor vehicle owner declines the service or requests that it be disabled; at that point, it can only be re-enabled if

service activation is requested via the in-vehicle On-Star button. It can also be disabled manually, in person, by altering the vehicle hardware.

OnStar is a conduit to communicate with GM vehicles. OnStar transmits vehicle system information—including information that a customer may use to determine the necessity for maintenance, diagnosis, or repair—to customers and to GM. The scope of these transmissions have expanded over time, and have changed as vehicle capabilities have changed. The information transmitted also varies by vehicle functionality and option packages. Further, based upon the diagnostic data transmitted by OnStar, GM can now make certain software fixes remotely to vehicle systems—including changes affecting vehicle functionality—by transmitting to the vehicle via the OnStar system. The information transmitted by OnStar includes (among other data) certain information regarding the vehicle's engine and propulsion systems, battery, transmission system, braking system, stability control, oil level, tire pressure, and air bags.

Persons with relevant knowledge regarding the provision of this data to vehicle owners or independent mechanics include:

- Jim Kelly, Program Engineering Manager at General Motors

This individual may be contacted through counsel for Plaintiff.

FCA

FCA customers may opt into or out of telematics service that transmits data externally from vehicles. FCA does not collect data from motor vehicles when their owners have opted out of service. Customers opt out of the service by contacting FCA or the service provider. In the case of VP4, that service provider is Sprint (now T-Mobile); in the case of VP4R, that service provider is Sirius XM's connectivity division; and in the case of TBM, that is FCA. Customers may not opt out of receipt of certain firmware update data (from FOTA, described below), but they can refuse the firmware updates that were transmitted.

FCA telematics units are conduits to communicate with the vehicles; they do not themselves collect any information used for diagnosis, maintenance, and repair. FCA telematics units externally transmit data that a customer may use to determine the necessity for

maintenance, diagnosis, and repair. This data is generated by the FCA vehicles' Service Quality Data Feed (SQDF), including data regarding mileage, emissions, tire pressure, trouble/error codes, engine performance, and fuel data. The SQDF sends immediate notifications regarding vehicle status to FCA, and it regularly collects vehicle status statistics that are sent in a monthly report to FCA, and then to customers via email. Customers also have an option to use a mobile application, UConnect Access, to receive data from the SQDF regarding current vehicle metrics, such as the odometer, fuel level, and tire pressure.

***** FOLLOWING PORTION OF RESPONSE TO INTERROGATORY NO. 5 CONFIDENTIAL *****

[redacted]

***** ABOVE PORTION OF RESPONSE TO INTERROGATORY NO. 5 CONFIDENTIAL *****

The customer is free to decide when to service the vehicle, at which point the vehicle's OBD system typically is accessed for vehicle data that is used to diagnose, repair and maintain the vehicle.

Persons with relevant knowledge regarding the provision of this data to vehicle owners or independent mechanics include:

- Andrew Baldino, FCA IT Connected Vehicle Concepts & Feasibility Lead
- Michael Braun, FCA Connect Vehicle Data Integration Lead

These individuals may be contacted through counsel for Plaintiff.

MBUSA

The wireless transmission function of all telematics units in vehicles distributed by MBUSA is capable of being disabled. For mbrace® units, customers may contact mbrace®

customer support and request that their units be disabled. mbrace® customer support can send a command to the vehicle that sets the device to "Out of Service" status, such that the device no longer communicates information from the vehicle. For Mmc units, customers can request that their authorized Mercedes-Benz dealer deactivate the unit, and that dealer can set the unit to "Out of Service" status.

Telematics units in vehicles distributed by MBUSA transmit certain vehicle status data, such as diagnostic trouble codes, maintenance conditions, engine performance, system temperatures, and fuel economy, that customers may use to determine if a vehicle requires diagnosis, repair, or maintenance.

Persons with relevant knowledge regarding the provision of this data to vehicle owners or independent mechanics include:

- Thomas Grycz

This individual may be contacted through counsel for Plaintiff.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 5

Subject to and without waiving the above objections, Auto Innovators supplements its response as follows:

TMNA

The wireless transmission function of all Service Connect telematics units can be disabled. If a customer wishes to disable Service Connect, the customer may contact Toyota via email or phone or utilize the Toyota or Lexus mobile application. Alternatively, the customer may press the "SOS" button in their motor vehicle, which will connect the customer with a call center. Once the customer informs Toyota that they wish to disconnect Service Connect, Toyota can disable the motor vehicle's data communication module (DCM) so that vehicle data is not transmitted.

Telematics units in TMNA vehicles transmit various vehicle data, such as fuel levels, vehicle speed, odometer information, "check engine" information, trouble codes, braking

information, and fuel injection volume, that may be used to determine if diagnosis, repair, or maintenance is required.

Persons with relevant knowledge regarding the provision of this data to vehicle owners or independent mechanics include:

- Mark McClung, Connected Vehicle Strategy and Business Development

This individual may be contacted through counsel for Plaintiff.

INTERROGATORY NO. 6

For each On-Board Diagnostic System Identified in response to Interrogatory No. 4:

a. State all categories of information "used for or otherwise related to the diagnosis, repair or maintenance of the vehicle" that are, or will be, collected by that On-Board Diagnostic System; and

b. Identify all Persons with knowledge Concerning the ways in which information collected by that On-Board Diagnostic System is, or will be, made accessible to vehicle owners or independent mechanics.

RESPONSE TO INTERROGATORY NO. 6

Auto Innovators specifically incorporates by reference the above Preliminary Statement and General Objections as if fully set forth herein. Auto Innovators further incorporates by reference its objections to Interrogatory no. 4, which are referenced in this Interrogatory, as well as its objections to Interrogatories nos. 2 and 3, which are referenced in Interrogatory no. 4. Auto Innovators further objects to this Interrogatory as overbroad, unduly burdensome, ambiguous, and vague because it requests "all" categories of information that are "used for or otherwise related to the diagnosis, repair or maintenance of the vehicle"—which apparently would include most data generated, stored in, or transmitted by a motor vehicle. Auto Innovators further objects to this Interrogatory as overbroad and unduly burdensome because it requests "all Persons" with knowledge concerning information from on-board diagnostics systems that would be made accessible to vehicle owners of independent mechanics—which apparently would include thousands of individuals. Auto Innovators further objects to this Interrogatory as vague and

ambiguous, as "On-Board Diagnostic System" is undefined and, to the knowledge of Auto Innovators, vehicles' on-board diagnostics functions are fully integrated into vehicle controls and do not constitute a separate unit. Auto Innovators further objects to this Interrogatory as overbroad as to time; Auto Innovators will only provide information related to model years 2018 to the present, as well as known information related to future model years through model year 2025. Auto Innovators further objects to this Interrogatory as compound, conjunctive, and disjunctive, and as containing subparts. Auto Innovators further objects to this Interrogatory to the extent the information in this Interrogatory may be provided to Defendant through other means, including in documents produced by Auto Innovators. Auto Innovators further objects to the extent it seeks information from the Designated Members beyond that designated in Auto Innovators' Initial Disclosures. Subject to and without waiving said objections, Auto Innovators responds as follows:

GM

GM's OBD systems vary in the data they collect from GM vehicles depending on the features and hardware of each vehicle. In addition, each vehicle's OBD systems are individually designed and calibrated to meet state and federal regulations. Even within a particular model, there can be significant differences in the diagnostic information due to the varying features and hardware on particular motor vehicles. The vehicle diagnosis, repair, or maintenance data measured by OBD systems include (among other data): engine data, exhaust data, brake system data, and fuel system data.

Persons with relevant knowledge regarding the provision of this data to vehicle owners or independent mechanics include:

- Erika Pruski, Global Technical Specialist for Onboard Diagnostics at General Motors
- Robert Stewart, Aftermarket Service Support at General Motors
- Dante Williams, Aftersales Data Licensing Manager at General Motors

These individuals may be contacted through counsel for Plaintiff.

FCA

The OBD system in FCA vehicles varies depending on the features of each vehicle, and each vehicle's OBD functions are individually designed and developed according to the features of each vehicle and any applicable regulations. Even within a particular model, there can be significant differences in the diagnostic information due to the varying features on particular motor vehicles. Each Electronic Control Unit (ECU) within a motor vehicle has its own OBD function. For example, the powertrain control module (PCM), transmission control module (TCM), body control module (BCM), occupant restraint controller (ORC), and anti-lock braking system (ABS) each have their own OBD function that provides data used for vehicle diagnosis, repair, or maintenance.

Persons with relevant knowledge regarding the provision of this data to vehicle owners or independent mechanics include:

- Bill Mazzara, Tech Fellow - EE&SW - Vehicle Cyber Security Governance & Strategy
- Kevin Jones, Manager of Production Operations

These individuals may be contacted through counsel for Plaintiff.

<u>**SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 6**</u>

Subject to and without waiving the above objections, Auto Innovators supplements its response as follows:

TMNA

The OBD systems in TMNA vehicles vary depending upon the features and hardware in each vehicle, and are designed to comply with federal and state regulations governing OBD systems. TMNA vehicles' OBD systems provide diagnostic, maintenance and repair information such as diagnostic trouble codes (DTCs), freeze frame data, and parameter IDs related to various motor vehicle systems, including the vehicles' powertrain, body, chassis, and safety systems.

Persons with relevant knowledge regarding the provision of this data to vehicle owners or independent mechanics include:

- David Stovall, Manager, Diagnostics and Telematics/Tools and Equipment at TMNA.

This individual may be contacted through counsel for Plaintiff.

INTERROGATORY NO. 18(a)[2]

Identify all acts that each Designated Member, Actively Participating Member, or Other Member has taken since 2015 toward complying with 42 U.S.C. § 7521(m)(5) and regulations promulgated pursuant to that subsection.

RESPONSE TO INTERROGATORY NO. 18(a)

Auto Innovators specifically incorporates by reference the above Preliminary Statement and General Objections as if fully set forth herein. Auto Innovators further objects to this Interrogatory because it requests information related to Auto Innovators members other than FCA, GM, MBUSA, or TMNA, and to the extent it seeks information from the Designated Members beyond that designated in Auto Innovators' Initial Disclosures, and thus is inappropriate for the reasons described in paragraph 11 of the General Objections above. Auto Innovators further objects to this Interrogatory because the acts taken by Auto Innovators' members to comply with 42 U.S.C. § 7521(m)(5) and regulations promulgated pursuant to that subsection are irrelevant to whether the 2020 Data Law is preempted. Auto Innovators further objects to this Interrogatory as overbroad and unduly burdensome because it seeks information related to "all" acts, for a six-year period, undertaken by all members of Auto Innovators. Subject to and without waiving said objections, Auto Innovators responds as follows:

GM

GM has taken measures to comply with 42 U.S.C. § 7521(m)(5) and regulations promulgated pursuant to that subsection by providing access to maintenance and emissions-related diagnostic information in accordance with Environmental Protection Agency regulations and pricing requirements. The pricing structure was prepared following a study by a third-party

---

[2] This Interrogatory was the first one of two designated by Defendants as "Interrogatory no. 18."

consultant; it is similar to the pricing provided to GM dealers, and was updated most recently in 2014. GM shares the use of its diagnostic tools with independent servicers; however, it does not share the cybersecurity protections that are used to make those tools secure.

FCA

FCA has complied with 42 U.S.C. § 7521(m)(5) and regulations promulgated pursuant to that subsection by:

- Making all the same service, wiring and diagnostic information used by dealership technicians available to the aftermarket technicians through TechAuthority.
- Making available their diagnostic scan tool, with the same diagnostic capabilities as dealerships.
- Making available their diagnostic scan tool software compatible with J2534 hardware to provide access to their OBD and repair information system.
- Making available their diagnostic scan tool vehicle-specific content information for the sole purpose of making third party scan tools (Snap-On, Bosch scan tools etc.).
- Setting up a third-party portal, called AutoAuth, to provide authorization to third-party repair shops that wish to be granted access to the FCA Security Gateway Module to perform authenticated diagnostics.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 18(a)

Subject to and without waiving the above objections, Auto Innovators supplements its response as follows:

TMNA

TMNA has complied with 42 U.S.C. § 7521(m)(5) and regulations promulgated pursuant to that subsection by:

- Making TMNA's technical information system, containing the same level of service information that dealers have, available to independent repair facilities via a website: TechInfo.

- Making the same special service tools and diagnostic tools that dealers have access to available to independent repair facilities.
- Following standardized reprogramming and diagnostics, *e.g.*, by using the J2534 reprogramming standard.
- Licensing TMNA data to service information providers and scan tool makers.

INTERROGATORY NO. 19

What is the earliest date by which, You contend, each Designated Member, Actively Participating Member, and Other Member can Comply With § 2 of the 2020 Right to Repair Law while also complying with the Motor Vehicle Safety Act, the Clean Air Act, and all currently-existing regulations promulgated under those laws?

RESPONSE TO INTERROGATORY NO. 19

Auto Innovators specifically incorporates by reference the above Preliminary Statement and General Objections as if fully set forth herein. Auto Innovators further objects to this Interrogatory because it is compound and conjunctive. Subject to and without waiving said objections, Auto Innovators responds as follows:

There is no date upon which FCA, GM, or MBUSA can comply with § 2 of the 2020 Data Law while also complying with the Vehicle Safety Act, the Clean Air Act, and currently existing regulations promulgated under those laws. In her "fair, concise summary," the Attorney General construes § 2 of the 2020 Data Law as requiring manufacturers to remove existing cybersecurity and/or access controls around vehicle systems to provide unfettered, standardized access to vehicle networks, on-board diagnostic systems, and mechanical data—the removal of which would compromise motor vehicle safety and emissions controls by allowing, among other things, third-party access to vehicle systems operating core vehicle functions such as acceleration, braking, and steering, as well as modules that help to ensure emissions performance. Those requirements are thus inconsistent with manufacturers' federal obligations, regardless of timing.

<u>SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 19</u>

Subject to and without waiving the above objections, Auto Innovators supplements its response as follows:

For the same reasons, there is no date upon which TMNA can sell motor vehicles that comply with § 2 of the 2020 Data Law while also complying with the Vehicle Safety Act, the Clean Air Act, and currently existing regulations promulgated under those laws.

<u>INTERROGATORY NO. 20</u>

What is the earliest date by which, You contend, each Designated Member, Actively Participating Member, and Other Member can Comply With § 3 of the 2020 Right to Repair Law while also complying with the Motor Vehicle Safety Act, the Clean Air Act, and all currently-existing regulations promulgated under those laws?

<u>RESPONSE TO INTERROGATORY NO. 20</u>

Auto Innovators specifically incorporates by reference the above Preliminary Statement and General Objections as if fully set forth herein. Auto Innovators further objects to this Interrogatory because it is compound and conjunctive. Subject to and without waiving said objections, Auto Innovators responds as follows:

There is no date upon which FCA, GM, or MBUSA can comply with § 3 of the 2020 Data Law while also complying with the Vehicle Safety Act, the Clean Air Act, and currently existing regulations promulgated under those laws. Compliance with § 3 of the 2020 Data Law would require manufacturers to remove existing cybersecurity and/or access controls around vehicle systems to provide unfettered, standardized access to vehicle networks, on-board diagnostic systems, and mechanical data—the removal of which would compromise motor vehicle safety and emissions controls by allowing, among other things, third-party access to vehicle systems operating core vehicle functions such as acceleration, braking, and steering, as well as modules that help to ensure emissions performance. Those requirements are thus inconsistent with manufacturers' federal obligations, regardless of timing.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 20

Subject to and without waiving the above objections, Auto Innovators supplements its response as follows:

For the same reasons, there is no date upon which TMNA can sell motor vehicles with telematics systems that comply with § 3 of the 2020 Data Law while also complying with the Vehicle Safety Act, the Clean Air Act, and currently existing regulations promulgated under those laws.

Date: March 9, 2021

Respectfully submitted,

Alliance for Automotive Innovation
By its attorneys,

/s/ John Nadolenco

John Nadolenco (*pro hac vice*)
Andrew J. Pincus (*pro hac vice*)
Erika Z. Jones (*pro hac vice*)
Archis A. Parasharami (*pro hac vice*)
Eric A. White (*pro hac vice*)
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
Tel: (202) 263-3000
jnadolenco@mayerbrown.com
apincus@mayerbrown.com
ejones@mayerbrown.com
aparasharami@mayerbrown.com
eawhite@mayerbrown.com

Laurence A. Schoen, BBO # 633002
Elissa Flynn-Poppey, BBO# 647189
Andrew N. Nathanson, BBO#548684
Mintz, Levin, Cohn, Ferris,
Glovsky, and Popeo, P.C.
One Financial Center
Boston, MA 02111
Tel: (617) 542-6000
lschoen@mintz.com
eflynn-poppey@mintz.com
annathanson@mintz.com

Charles H. Haake (*pro hac vice*)
Jessica L. Simmons (*pro hac vice*)
Alliance for Automotive Innovation
1050 K Street, NW
Suite 650
Washington, DC 20001
Tel: (202) 326-5500
chaake@autosinnovate.org
jsimmons@autosinnovate.org

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION, Plaintiff, v. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendant.	CIVIL ACTION NO. 1:20-cv-12090-DPW

VERIFICATION

I, CHARLES HAAKE, am the Vice President and General Counsel of Alliance For Automotive Innovation ("Auto Innovators"). I have the authority to execute this Verification on behalf of Plaintiff Auto Innovators. I have reviewed the contents of Plaintiff Alliance for Automotive Innovation's Responses to Attorney General Maura Healey's First Set of Interrogatories. To the best of my knowledge, Auto Innovators' responses in the foregoing document are accurate and truthful as of the day they are made.

I verify under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 9th day of March 2021, in Washington, DC.

Charles Haake

CERTIFICATE OF SERVICE

I, Daniel Queen, hereby certify that on March 9, 2021, the foregoing document was served on counsel for the defendant by electronic mail.

/s/ Daniel Queen
Daniel Queen

The remaining Exhibits referenced in this affidavit — Exhibits 6, 7, 8, 9, 11, 12, 504, 514, 515, and Def.'s Exhibit H — have been marked confidential and filed under seal in accordance with the Confidentiality Protective Order (ECF #91) in this case.